Last updated: 20 May 2021

Global Binding Corporate Rules:

Controller Policy

Contents

INTRODUCTION

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

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

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

This Controller 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, 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 third party, that organization is deemed to be a "*processor*" of the information. In this case, the relevant controller of the personal information (i.e. the relevant third party) 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 EEA that do not ensure an adequate level of data protection. Some of the countries in which Avaya operates are not regarded by EEA data protection authorities 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 Controller 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.

SCOPE OF THIS CONTROLLER POLICY

The standards described in this Controller Policy are worldwide standards that apply to all Group Members when processing any personal information as a controller. As such, Sections A and B of this Controller 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 in the EEA and then transferred to a Group Member outside the EEA.

This Controller Policy applies to all personal information that Avaya is processing for purposes of carrying out its business activities, employment administration and supplier chain management. As such, the personal information to which this Controller Policy applies includes:

- human resources data including personal information of Avaya's past and current employees, individual consultants, independent contractors, temporary staff and job applicants;
- supply chain management data including data about Avaya's vendors, suppliers and other third party service providers;

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

- customer relationship management data about Avaya's customers (both individual consumers and business customers);
- content data uploaded by Avaya customers (individual consumers only, not business customers); and
- customer file metadata (to the extent this comprises personal information),

(collectively, "**Avaya Personal Data**"). More details about the material scope of this Controller Policy are provided in Appendix 10.

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

LEGALLY BINDING EFFECT OF THIS CONTROLLER POLICY

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

All Group Members who process personal information as a controller must comply with the Rules set out in **Part II** of this Controller Policy together with the policies and procedures set out in the appendices in **Part III** of this Controller Policy. The procedures and appendices are an integral part of this Controller Policy.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Controller Policy, your rights under this Controller 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 Controller Policy are notified to the Group Members 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: CONTROLLER OBLIGATIONS

This Controller Policy applies in all situations where a Group Member processes personal information as a controller.

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

- Section A addresses the basic data protection principles that Avaya must observe when it processes personal information as a controller.
- Section B deals with certain practical data protection commitments made by Avaya in connection with this Controller Policy.
- Section C describes the third party beneficiary rights that Avaya grants to individuals in its capacity as a controller under this Controller 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 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 Controller Policy, Avaya will process personal information in accordance with the Rules in this Controller Policy.

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

Avaya will ensure all processing of personal information 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.

RULE 2 – FAIRNESS AND TRANSPARENCY

Rule 2 – Avaya will inform and explain to individuals, at the time when their personal information is collected, how their personal information will be processed.

1. Information that must be provided to individuals

Avaya will ensure that individuals are told in a clear and comprehensive way how their personal information will be processed (usually by means of an easily accessible fair processing statement). The information Avaya has to provide to individuals includes all information necessary in the circumstances to ensure that the processing of personal information is fair, including the following:

- the **identity** of the controller and its contact details;
- the contact details of the **Data Protection Officer** ;
- information about an **individual's rights** to request access to, rectify, or erase their personal information, as well as the right to restrict or object to processing, and the right to data portability;
- the **purposes** of the processing for which the personal information are intended as well as the legal basis for the processing;
- where the processing is based on Avaya's or a third party's legitimate interests, the **legitimate interests** pursued by Avaya or by the third party;
- the **recipients** or categories of recipients of their personal information;
- where processing is based on **consent**, the right to withdraw that consent at any time without affecting the lawfulness of processing based on consent before its withdrawal;
- whether the controller intends to **transfer** personal data to a third country and reference to the suitable safeguards (i.e., this Controller Policy) and the means by which to obtain a copy;
- the **retention period** of their personal information or the criteria used to determine the retention period;
- the right to **lodge a complaint** with the data protection authorities in the EEA;
- whether the provision of personal information is a **statutory or contractual requirement**, as well as whether the individual is obliged to provide the personal information and of the possible consequences of failure to provide such data; and
- the existence of **automated decision-making**, including profiling, and where such decisions produce a legal effect or may significantly affect the individuals whose personal information are processed in this way, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

Where the personal information are not obtained directly from the individual concerned, Avaya shall provide those individuals, in addition to the information above, with the following information:

- the **categories** of Personal Information that are being Processed; and
- from which **source** the Personal Information originates, and if applicable, whether it came from publicly accessible sources.

2. Moment when individuals must be informed

Where personal information are obtained from the individuals, Avaya shall provide the individuals with the above information at the time when such personal information are obtained.

Where personal information are not obtained directly from the individuals Avaya shall provide the above information to the individuals (1) within a reasonable period of time after obtaining their personal information, but at the latest within one month, having regard to the specific circumstances in which the personal information are processed; or (2) if the personal information are to be used for communication with the individuals, at the latest at the time of the first communication to those individuals; or (3) if a disclosure to another recipient is envisaged, at the latest when the personal information are first disclosed.

3. Exceptions to the obligation to inform individuals

Where personal information are obtained from the individuals, Avaya may be exempt from providing the above information to those individuals if they already have the information.

Where personal information are not obtained directly from the individuals, Avaya may be exempt from providing this information to individuals where: (1) the individuals already have the information; or (2) providing the information may prove impossible or involve a disproportionate effort; or (3) as otherwise permitted by Applicable Data Protections Laws. Where this is the case, Avaya's Data Privacy Stewards will decide what course of action is appropriate to protect the individual's rights, freedoms and legitimate interests and will inform Avaya's Data Protection Officer accordingly.

Where Avaya processes personal information for the purposes described in Part I of this Controller Policy, Avaya will be the controller of that information. On the other hand, where Avaya is processing personal information on behalf of a controller, it will comply with the requirements of the Binding Corporate Rules: Processor Policy.

RULE 3 – PURPOSE LIMITATION

Rule 3A – Avaya will only obtain and process personal information for those purposes which are known to the individual or which are within their expectations and are relevant to Avaya.

Rule 1 above provides that Avaya will comply with any applicable legislation relating to the collection of personal information. This means that where Avaya collects personal information in the EEA and local law requires that Avaya may only process it for specific, legitimate purposes, and not use that personal information in a way that is incompatible for those purposes, Avaya will honour these obligations.

Under Rule 3A, Avaya will identify and make known to the individuals from whom it collects personal information the purpose(s) for which their personal information will be processed when such information is obtained from them.

Rule 3B – Avaya will only process personal information for specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those purposes unless such further processing is consistent with the applicable law of the country in which the personal information was collected.

If Avaya collects personal information for a specific purpose in accordance with Rule 1 (as communicated to the individual via the relevant fair processing statement) and subsequently Avaya wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change unless it is within their expectations and they can express their concerns or there is a legitimate basis for not doing so consistent with the applicable law of the country in which the personal information was collected.

In certain cases, for example, where the processing is of sensitive personal information, or Avaya is not satisfied that the processing is within the reasonable expectation of an individual, Avaya will obtain the individual's consent before processing that information for a different purpose.

RULE 4 – DATA MINIMIZATION AND ACCURACY

Rule 4A – Avaya will keep personal information accurate and up to date.

Avaya will take reasonable steps to ensure that all personal information that is inaccurate, having regard to the purposes for which it is processed, will be erased or rectified without delay.

In order to ensure that the personal information held by Avaya is accurate and up to date, Avaya actively encourages individuals to inform Avaya when their personal information has changed or has otherwise become inaccurate.

Rule 4B – Avaya will only process personal information that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Avaya will identify the minimum amount of personal information necessary in order to properly fulfil its purposes.

Avaya shall implement appropriate technical and organizational measures, which are designed to implement the protection of personal information into the processing that is carried out by Avaya.

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

Rule 5 – Avaya will only keep personal information for as long as is necessary for the purposes for which it is collected and further processed.

Avaya will comply with Avaya's record retention policies and guidelines as revised and updated from time to time and will inform individuals how long their data is retained in accordance with Rule 2 above.

RULE 6 – SECURITY, INTEGRITY AND CONFIDENTIALITY

Rule 6A – Avaya will implement appropriate technical and organizational measures to ensure a level of security of personal information that is appropriate to the risk for the rights and freedoms of the individuals.

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.

To this end, Avaya will comply with the requirements in the security policies in place within Avaya, as revised and updated from time to time, together with any other security procedures relevant to a business area or function.

Avaya will ensure that any employee of Avaya who has access to personal information will do so on instructions from Avaya.

Rule 6B – Avaya will ensure that providers of services to Avaya also adopt appropriate and equivalent security measures.

Where a Group Member appoints an internal or external service provider to process personal information on its behalf, Avaya must impose strict contractual terms, in writing, on the service provider that require it to:

- act only on Avaya's instructions when processing that information, including with regard to international transfers of personal information;
- ensure that any individuals who have access to the data are subject to a duty of confidentiality;
- have in place appropriate technical and organizational security measures to safeguard the personal information;
- only engage a sub-processor if Avaya has given its prior specific or general written authorisation, and on condition the sub-processor agreement protects the personal information to the same standard required of the service provider;

- assist Avaya in ensuring compliance with its obligations as a controller under applicable data protection laws, in particular with respect to reporting data security incidents under Rule 6C and responding to requests from individuals to exercise their data protection rights under Rule 7A;
- return or delete the personal information once it has completed its services; and
- make available to Avaya all information it may need in order to ensure its compliance with these obligations.

Rule 6C – Avaya will comply with data security breach notification requirements as required under applicable law.

In case of a security incident that affects the personal information that is being processed, Avaya will review the nature and seriousness of the data security incident and determine whether it is necessary under Applicable Data Protection Laws to notify:

- the competent data protection authorities because the incident is likely to create a **risk** for the rights and freedoms of individuals affected by the incident; and,
- where applicable, the individuals affected by the security incident, because the incident creates a high risk for their rights and freedoms in accordance with applicable law.

Avaya's Data Breach Incident Response Team shall document all data security incidents (including the facts relating to such incident, its effects and the remedial action taken) and shall make such documentation available to the competent data protection authorities upon request.

The Data Protection Officer shall be responsible for ensuring that any such notifications, where necessary, are made in accordance with the requirements of, and timescales specified by, Applicable Data Protection Laws, which (in the case of the GDPR) shall mean notifying the competent data protection authorities in the EEA without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the incident. Where notification to the affected individuals is also required, they must be notified without undue delay.

RULE 7 – RIGHTS OF INDIVIDUALS

Rule 7A – Avaya will adhere to the Data Subject Rights Procedure and will respond to any requests from individuals to access their personal information in accordance with applicable law.

Individuals may ask Avaya to provide them with access to, and a copy of, the personal information Avaya holds about them (including information held in both electronic and paper records). Avaya will follow the steps set out in the Data Subject Rights Procedure (see Appendix 2) when dealing with such requests.

Rule 7B – Avaya will also deal with requests to rectify or erase personal information, to exercise the right to data portability, to restrict or to object to the processing of personal information in accordance with the Data Subject Rights Procedure.

Individuals may ask Avaya to rectify or erase personal information Avaya holds about them. In certain circumstances, individuals may also exercise their right to data portability, restrict the processing or object to the processing of their personal information. Avaya will follow the steps set out in the Data Subject Rights Procedure (see Appendix 2) in such circumstances.

RULE 8 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

Rule 8 – Avaya will not transfer personal information to third parties outside the EEA without ensuring adequate protection for the information in accordance with the standards set out by this Controller Policy.

In principle, transborder transfers of personal information to third parties[4] outside the Avaya group of entities are not allowed without appropriate steps being taken, such as signing up to contractual clauses, which will protect the personal information being transferred.

No Group Member may transfer personal information internationally unless and until such measures as are necessary to comply with Applicable Data Protection Laws governing international transfers of personal information have been satisfied in full, including with respect to onward transfers of personal information from a third country.

For the avoidance of doubt, this Rule 8 also pertains to onward transfers of Personal Information to controllers and processors that are not Group Members.

RULE 9 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 9 – Avaya will only process sensitive personal information where the individual's explicit consent has been obtained, unless Avaya has an alternative legitimate basis for doing so consistent with the applicable law of the country in which the personal information was collected.

Avaya will assess whether sensitive personal information is required for the intended purpose of the processing. Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural purpose, data concerning health, or data concerning an individual's sex life or sexual orientation.

In principle, Avaya must obtain the individual's explicit consent to collect and process his/her sensitive personal information, unless Avaya is otherwise required to do so by applicable law or has another legitimate basis for doing so consistent with the laws of the country in which the personal information was collected. Consent must be given freely and must be specific, informed and unambiguous.

RULE 10 – LEGITIMISING DIRECT MARKETING

Rule 10 – Avaya will allow customers to opt-out of receiving marketing information.

All individuals have the right to object, free of charge, to the use of their personal information for direct marketing purposes and Avaya will honour all such opt-out requests.

RULE 11 – AUTOMATED INDIVIDUAL DECISIONS INCLUDING PROFILING

Rule 11 – Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, and to contest such decision.

Avaya will not take any decision based solely on the automated processing of an individual's personal information, which produces legal effects concerning that individual, or significantly affects that individual,

[4] Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

unless such automated processing is authorized by law and measures are taken to protect the legitimate interests of the individual. Where such decisions are made, individuals will have the right to know the logic involved in the decision and may contest such decisions.

RULE 12 – ACCOUNTABILITY

Rule 12 A – Avaya will carry out a data protection impact assessment when the processing is likely to result in a high risk for the individuals concerned.

Where the processing is likely to result in a high risk to the rights and freedoms of individuals, Avaya shall, prior to the processing, assess the impact of the envisaged processing operations on the protection of personal data, taking into account the nature, scope, context and purposes of the processing.

Avaya shall seek the advice of the Data Protection Officer and where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk, Avaya will consult the competent data protection authority[5] prior to the processing.

Rule 12 B – Avaya will maintain records of data processing activities under its responsibility.

Each Group Member shall maintain a record of the processing activities under its responsibility and will make them available to the competent data protection authorities upon request.

Rule 12 C – Avaya shall implement Privacy by Design and Privacy by Default for new systems and applications.

Avaya shall at the time of the determination of the means of the processing and at the time of the processing itself, implement appropriate technical and organizational measures which are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards into the processing.

In addition, Avaya shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

SECTION B: PRACTICAL COMMITMENTS

RULE 13 – STAFF AND SUPPORT

Rule 13 – 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 Controller Policy supported by Privacy Stewards at regional, country and business unit level who are responsible for overseeing and enabling compliance with this Controller 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

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

with Applicable Data Protection Laws and the Controller Policy. The group DPO also reports issues directly to Avaya's independent audit committee.

All Group Members acting as controllers must comply, and be able to demonstrate compliance, with this Controller Policy.

RULE 14 – PRIVACY TRAINING

Rule 14 – 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 15 – AUDIT

Rule 15 – Avaya will verify compliance with this Controller 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 Controller Policy (including methods of ensuring that corrective actions will take place). 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 Controller Policy (including any related procedures and controls) in accordance with the Cooperation Procedure (see Appendix 7).

RULE 16 – COMPLAINT HANDLING

Rule 16 – 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 Controller 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 17 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 17 – Avaya will cooperate with the data protection authorities on any issue related to the Controller Policy in accordance with the Cooperation Procedure set out in Appendix 7.

Avaya will cooperate with the competent data protection authorities by complying with the Cooperation Procedure set out in Appendix 7 and will abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Controller 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 18 – UPDATE OF THE CONTROLLER POLICY

Rule 18– Avaya will report changes to this Controller Policy to the data protection authorities in accordance with the Updating Procedure set out in Appendix 8.

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

RULE 19 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE CONTROLLER POLICY

Rule 19A – Avaya will ensure that where it believes that the legislation applicable to it may prevent it from fulfilling its obligations under this Controller Policy or such legislation has a substantial effect on its ability to comply with this Controller Policy, Avaya will promptly inform the Data Privacy Officer and the EU entity with data protection responsibilities, unless otherwise prohibited by a law enforcement authority.

Rule 19B – Avaya will ensure that where there is a conflict between the legislation applicable to it and this Controller Policy, the Data Privacy Officer will make a responsible decision on the action to take and will report to the data protection authority with competent jurisdiction in case of doubt.

RULE 20 – GOVERNMENT REQUESTS FOR DISCLOSURE OF PERSONAL INFORMATION

If a Group Member receives a legally binding request for disclosure of personal information by a law enforcement authority or state security body that is subject to this Controller Policy, it must comply with the Government Data Request Procedure set out in 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 controller (an "**EEA Entity**") and/or transferred to a Group Member located outside the EEA under this Controller 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 16, 17 and 19 under section B of Part II of this Controller Policy.

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

- *Complaints*: Individuals may submit complaints to an EEA Entity in accordance with the Complaint Handling Procedure (set out in Appendix 6) and may also 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 Controller Policy have been infringed as a result of the processing of their personal information in non-compliance with this Controller Policy. Individuals may bring proceedings to enforce compliance with this Controller 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 Controller 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 Controller Policy have the right to receive compensation from the Controller or Processor for the damage suffered. In particular, in case of non-compliance with this Controller Policy by a non-EEA entity, 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 Controller Policy, in accordance with the determination of the court or other competent authority; and

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

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 Controller 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 Controller 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 Controller 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 Controller 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 Controller Policy.

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 CONTROLLER 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
Avaya Comunicacion Espana S. L. U.	Paseo de la Castellana 216, Madrid, 28046, Spain

Name of entity	Registered address
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
Avaya India Private Limited (Bangladesh Branch Office)	Faruque Rupayan Tower (18th Floor), Kemal Ataturk Avenue, Banani C/A, Dhaka, 1213, Bangladesh

Name of entity	Registered address
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
CAAS Technologies LLC	c/o Avaya, 350 Mt Kemble Avenue, PO BOX 1934, Morristown, New Jersey, 07960, United States of America

Name of entity	Registered address
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 Controller Policy() safeguards personal information transferred between Avaya's Group Members.

1.2 Individuals whose personal information is processed by Avaya under the Controller 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 deals with a Request it receives from individuals whose Personal Information are Processed as a Controller and are transferred under the Controller Policy.

1.4 Where a Request is subject to EEA data protection law 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 Avaya is entitled to the following rights:

(a) **Right to information**: this is the right to be informed about the processing of personal information by Avaya, 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 Avaya 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 a 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 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 then where Avaya is the Controller of that individual's personal information under this Controller Policy, it must help the individual to exercise his or her data protection rights directly in accordance with this Procedure.

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 then determine whether the Request has been made validly under applicable data protection laws and whether confirmation of identity, or any further information, is required in order to fulfil the Request; 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 Binding Corporate Rules: Processor Policy and the contract terms with that Controller, and will not respond to the Request directly unless authorised to do so by the Controller.

5. Response to a Request

5.1 If the Data Privacy Core Team has assessed that Avaya is the Controller of the personal information that is the subject of the Request, it will then contact the individual in writing to confirm receipt of the Request.

5.2 If Avaya is unable to identify the individual who has made the Request, it shall inform that individual, (to the extent possible) and shall put the Request on hold until the individual concerned provides additional information enabling his or her identification. If, despite Avaya's request for additional information, it is still unable to identify that individual, in such case Avaya will not be obliged to respond to the Request.

5.3 The Request must generally be made in writing[6], including by electronic means, unless the Request can be made orally in accordance with applicable laws.

5.4 The Request does not have to be official or mention data protection law to qualify as a valid Request.

5.5 Avaya shall respond to Request in a concise, transparent, intelligible and accessible form. The information shall be provided in writing, or by other means. Where the individual has made the Request by electronic means, the information shall be provided including by electronic means, unless otherwise requested by the individual. When requested by the individual, Avaya shall provide the information orally, provided that the identity of the individual is proven by other means.

[6] Unless the local data protection law provides that an oral request may be made, in which case Avaya will document the request and provide a copy to the individual making the request before dealing with it.

5.6 Avaya must respond to a Request without undue delay and in any case no later than one month of receipt of that request. That period may be extended by two further months where necessary, taking in account the complexity or number of Requests. Whenever Avaya decides to extend the period of response, it shall inform the individual who has made a Request of any extension within one month of receipt of the Request, together with the reasons for the delay.

5.7 Avaya shall not refuse to act on a Request unless Avaya can demonstrate that it is not in the position to identify the individuals who is making the Request or Avaya can demonstrate that the Request is manifestly unfounded or excessive (e.g. due to its repetitive character).

6. Requests for access to Personal Information

6.1 *Overview*

6.1.1 An individual has the right to obtain from Avaya confirmation as to whether or not personal information concerning him or her are being processed, and, where that is the case, access to more detailed information about the processing, including the purposes of the processing, the categories of personal information concerned, the recipients or categories of recipient to whom the personal information have been or will be disclosed, in particular recipients outside the EEA and, where possible, the envisaged period for which the personal information will be stored, or, if not possible, the criteria used to determine that period.

6.1.2 An individual is also entitled to request a copy of his or her personal information from Avaya in intelligible form ("**Access Request**").

6.2 *Exemptions to an Access Request*

6.2.1 An Access Request may be refused on the following grounds:

(a) the refusal to provide the information or carry out the Access Request of the individual is consistent with the exemptions under current EEA data protection law;

(b) the personal information is held by Avaya in non-automated form that is not or will not become part of a filing system; or

(c) the personal information does not originate from the EEA, has not been processed by any EEA Group Member, and the provision of the personal information requires Avaya to use disproportionate effort.

6.2.2 Avaya's Data Privacy Core Team will assess each Request individually to determine whether any of the above-mentioned exemptions applies.

6.3 *Avaya's search and the response*

6.3.1 Avaya's Data Privacy Core Team will arrange a search of all relevant electronic and paper filing systems.

6.3.2 Avaya's Data Privacy Core Team may refer any complex cases to the Data Privacy Officer for advice, particularly where the Request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.

6.3.3 The information requested will be collated by Avaya's Data Privacy Core Team into a readily understandable format (internal codes or identification numbers used at Avaya that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by Avaya's Data Privacy Core Team which includes information required to be provided in response to a data subject's access Request.

7. Requests for erasure, rectification, restriction of or objection to processing of personal information or to data portability

7.1 If a Request is received for the erasure or rectification of personal information, the restriction of or objection to processing or to data portability of an individual's personal information where Avaya is the Controller for that personal information, such a Request must be considered and dealt with as appropriate by Avaya's Data Privacy Core Team.

7.2 If a Request is received advising of a change in an individual's personal information where Avaya is the Controller for that personal information, such information must be rectified or updated accordingly.

7.3 When Avaya rectifies, erases or ports personal information, in its capacity as Controller 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.

7.4 If a Request is made to Avaya as a Controller to restrict or object to processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by Avaya, or on the basis of other compelling legitimate grounds, the matter will be referred to Avaya's Data Privacy Core Team to assess. Where the processing undertaken by Avaya is required by law, the Request will not be regarded as valid.

8. Questions about this Procedure

8.1 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

1.1 Avaya's compliance with global data protection laws and the Controller Policy are 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

2.1 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 Controller 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.

2.2 The DPO's key responsibilities include:

- Ensuring that the Controller Policy and other privacy related policies, objectives and standards are defined and communicated.
- Providing clear and visible senior management support and resources for the Controller Policy and for privacy objectives and initiatives in general.
- Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Controller 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 Controller Policy and related privacy and information protection strategies, policies and practices.
- Facilitating communications on the Controller 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

3.1 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 Controller 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 collection and use of personal information subject to the Controller Policy and to assess, in conjunction with the Business Data Privacy Stewards, the collection and use of personal information by Avaya's Group Members for potential privacy-related risks.

- Responding to inquiries and compliance relating to the Controller 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 Controller 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 Controller 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 Controller Policy and Avaya's related policies and business practices.

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

- Promoting the Controller 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 Controller Policy to the DPO.

- Ensuring that the commitments made by Avaya in relation to updating, and communicating updates to the Controller 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.

3.2 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 Controller 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 Controller 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.

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

4. Privacy Committee

4.1 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:

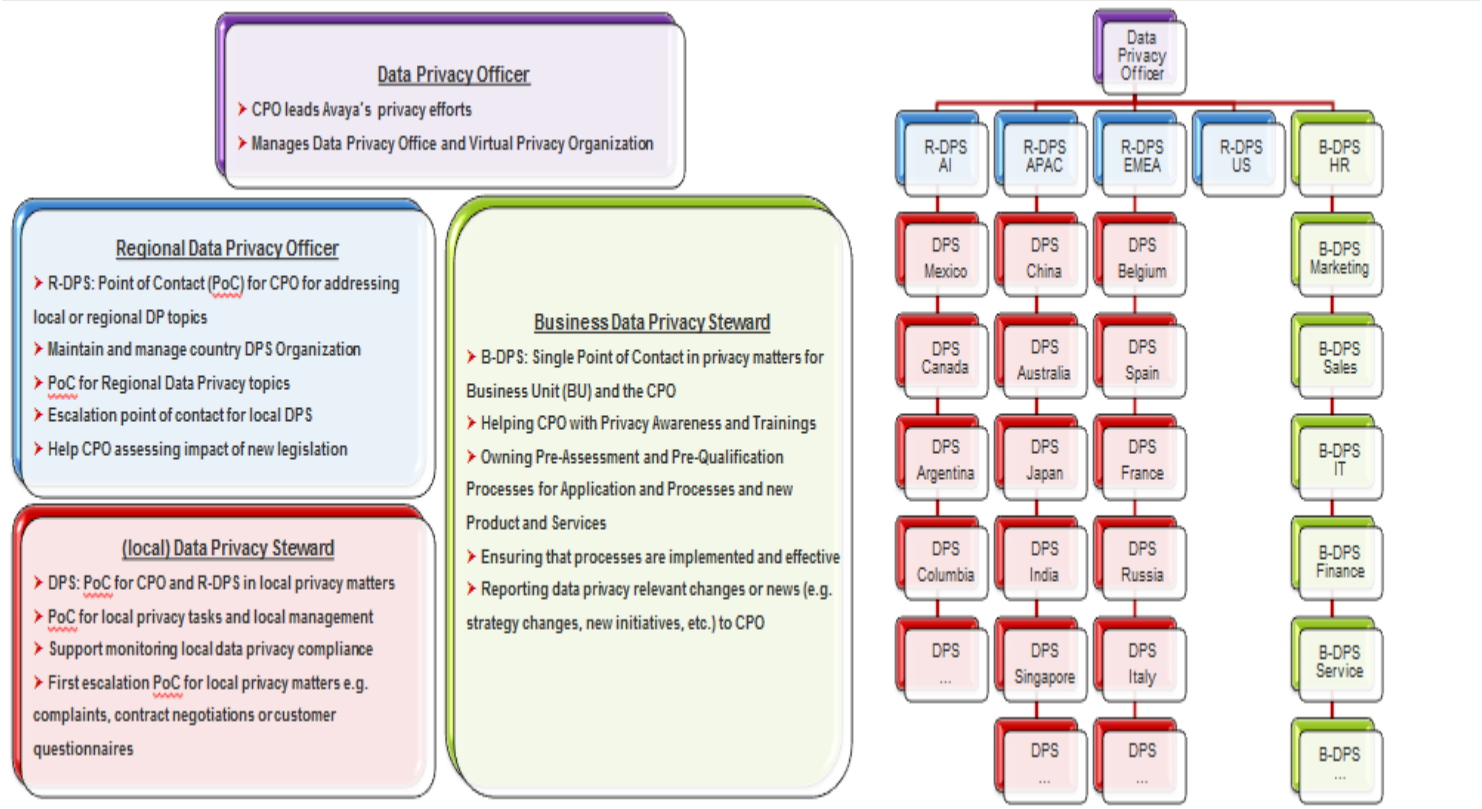
- Promoting the Controller Policy at all levels in their functional areas.
- Implementing Avaya's privacy policies (including the Controller Policy) within their respective areas of responsibility and assisting the Data Privacy Core Team with its enforcement.
- Escalating questions and compliance issues or communicating any actual or potential violation of the Controller 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.

4.2 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.

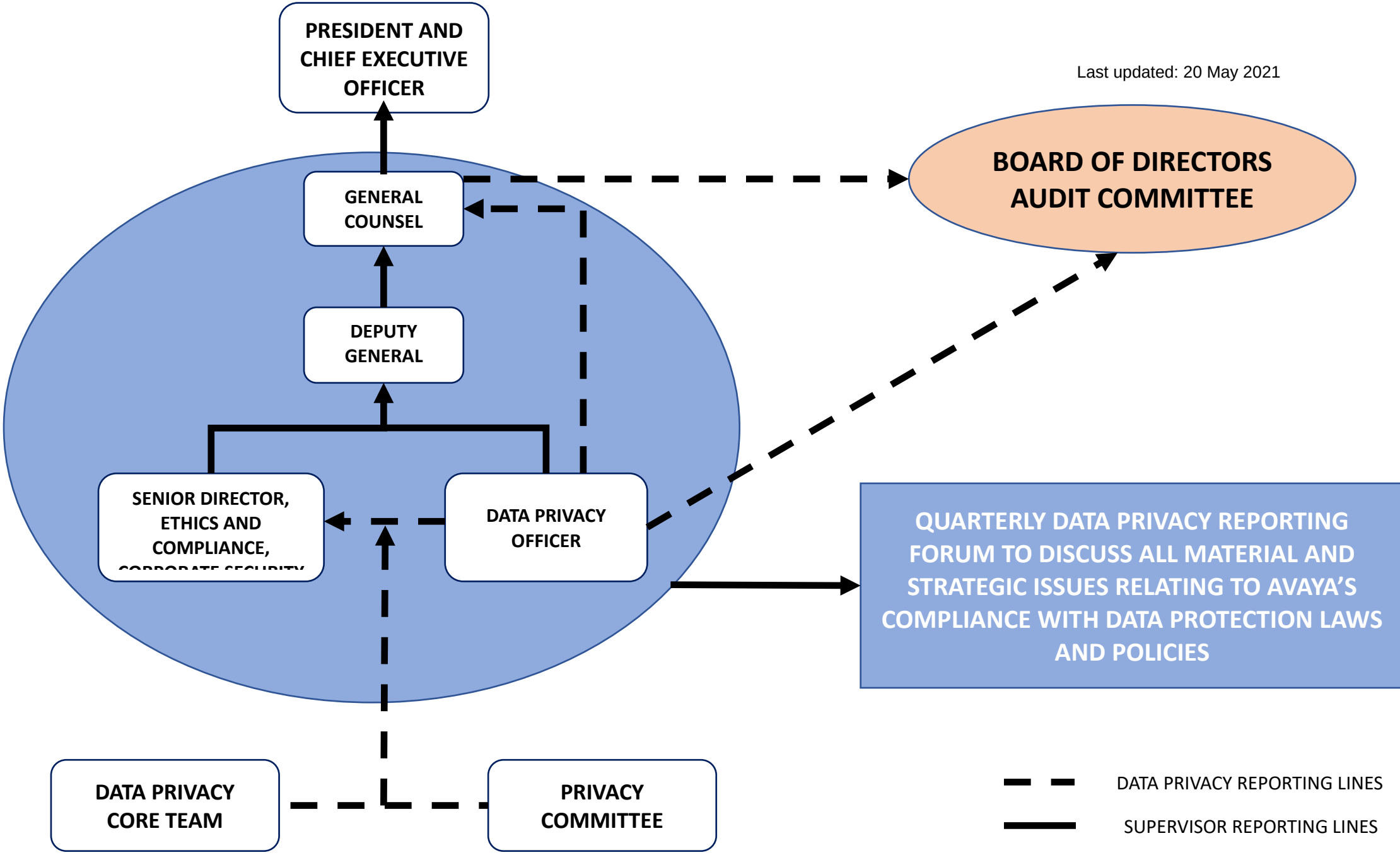
5. Avaya's Personnel

5.1 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 Controller 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



Last updated: 20 May 2021



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 Controller 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 Controller 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 Controller 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 Controller Policy

4.1 Avaya's training on the Controller 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 Controller Policy.

(d) Terminology and concepts.

4.1.2 The Controller Policy:

(a) An explanation of the Controller Policy.

(b) Practical examples.

(c) The rights that the Controller Policy give to individuals.

(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 Controller 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 Controller 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 Controller 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 Controller 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 Controller Policy as required by the data protection authorities, this is only one way in which Avaya ensures that the provisions of the Controller Policy are observed and corrective actions taken as required.

2. Approach

Overview of audit

2.1 Compliance with the Controller 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 Controller Policy and coordinating responses to audit findings as explained in Appendix 3.

Avaya's Internal AuditTeam is responsible for performing and/or overseeing independent audits of compliance with the Controller Policy and will ensure that such audits address all aspects of the Controller 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.

Frequency of audit

2.2 Audits of compliance with the Controller Policy are conducted:

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

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

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

Scope of audit

2.3 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.

Auditors

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

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

Reporting

2.6 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.

2.7 Upon request and subject to applicable law, Avaya will provide copies of the results of data privacy audits of the Controller Policy (including any related procedures and controls) to a competent EEA data protection authority.

Avaya's Data Privacy Core Team is responsible for liaising with the data protection authorities in the EEA 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 Controller Policy are dealt with.

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

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 Controller 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 authorities in the EEA in relation to the Controller Policy.

2. Cooperation Procedure

2.1 Where required, Avaya will make the necessary personnel available for dialogue with an EEA data protection authority in relation to the Controller Policy.

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

(a) any decisions made by relevant EEA data protection authorities on any data protection law issues that may affect the Controller Policy; and

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

2.3 Subject to applicable law, Avaya will provide upon request copies of the results of any data protection audit of the Controller Policy to a relevant EEA data protection authority.

2.4 Avaya agrees that:

(a) a competent EEA data protection authority may audit any Group Member located within its jurisdiction for compliance with the Controller 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 that jurisdiction; and

(b) a competent EEA data protection authority may audit any Group Member who processes personal information on behalf of a Controller established within the jurisdiction of that EEA data protection authority for compliance with the Controller 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).

Avaya agrees to abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Controller 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 Controller Policy to the data protection authorities in the EEA, individual data subjects, and to the Group Members bound by the Controller 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 Controller Policy

2.1 Avaya will communicate any material changes to the Controller 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 Controller Policy without undue delay to the Lead Data Protection Authority and to any other relevant EEA data protection authorities as appropriate.

3. Administrative changes to the Controller Policy

3.1 Avaya will communicate changes to the Controller 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 EEA data protection authorities (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 Controller Policy.

4. Communicating changes to the Controller Policy

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

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

(b) systematically to individuals who benefit from the Controller 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 Controller Policy. This information will be available on request from Avaya at dataprivacy@avaya.com.

5. Logging changes to the Controller Policy

5.1 The Controller 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 Controller Policy.

5.2 Avaya will also maintain an accurate and up-to-date list of all Group Members that are bound by the Controller 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 Controller 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 ("**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 For that reason, unless it is legally compelled to do so, Avaya will report to the competent data protection authorities in order 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 to the competent data protection authorities

4.1 Avaya will 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 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

6.2 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.

7. Queries

7.1 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 Controller Policy

1. Background

1.1 Avaya's Controller 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 Controller 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. Human Resources ("HR") 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 control 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 control described in this section to every Avaya Group Member inside and outside of the EEA.
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 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 inside and outside of the EEA.
What categories of personal information are transferred?	- **Identification data** – name, gender, photograph, date of birth, employee IDs. - **Contact details** – home and business address, telephone/email addresses, emergency contact details. - **Employment details** – job title/position, office location, employment contract, performance and

	disciplinary records, grievance procedures, sickness/holiday records. - **Background information** – academic/professional qualifications, education, CV/résumé. - **National identifiers** – national ID/passport, immigration/visa status, social security numbers. - **Spouse and dependent information, marital status**. - **Financial information** – banking details, tax information, withholdings, salary, benefits, expenses, company allowances, stock and equity grants. - **IT information** – information required to provide access to Avaya's IT systems and networks such as IP addresses, log files and login information. - **Any other information provided voluntarily by staff members** on their company profiles. - **Statistical information** about staff members. - **Background checks** (such as criminal records) where justified and in accordance with applicable laws.
What categories of sensitive personal information (if any) are transferred?	As a general rule, Avaya does not transfer any sensitive personal information relating to its staff members unless it is required to do so under applicable law. In such a case, Avaya may exceptionally transfer some information about: - a staff member's racial/ethnic origin, religion, gender and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; or - a staff member's physical or mental condition to provide work-related accommodations, health and insurance benefits to you and your dependents, or to manage absences from work.
Who are the types of individuals whose personal information are transferred?	Avaya's staff members and job applicants.

Why is this personal information transferred and how will it be used?	Avaya may transfer this personal information within the group in order to manage human resources at a group level, as well as for other processing activities such as compliance with applicable laws and regulations, training/development, IT services/security, audit and necessary investigations, tax and accounting, and general business management. In particular, the personal information may be used for the following purposes: - recruitment - talent management and organizational development (e.g., resource optimization, etc.) - payroll, wages and salaries, salary market analysis, bonuses, equity grants (for stock and benefits plans administration) - administration of healthcare, compensation, incentives programs and other benefits - work-related injury and illness, absences, including the management of employee health and safety, and disabilities - career planning, appraisals and performance management - international mobility (e.g., relocation) - training/development, e-learning - office management and employee support services (e.g. mobile phones, computers) - business travel management and expense reimbursement - emergency business continuity procedure - management of company car fleet - IT support services and IT security/management (please see our Global IT/Security Policy for more detail) - telephone recordings for employee trainings and quality of service - accounting, financial planning, internal audit, internal surveys and statistics - disciplinary matters, internal investigations, anonymous hotline

	- to help Avaya conduct its business more effectively and efficiently – for example, for general HR resourcing on a global level
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 and external processors are located. A list of Avaya Group Member locations is available at Appendix 1.

3. Customer relationship 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 control 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 control described in this section to every Avaya Group Member inside and outside of the EEA.
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 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 inside and outside of the EEA.
What categories of personal information are transferred?	- **Identification data** –name, and date of birth. - **Contact details** – address, telephone, email address, etc. - **Professional details** – job title/position, affiliated organization, office location, etc. - **Financial details** – bank account number, credit worthiness, and credit card details. - **National identifiers** – tax ID and VAT number. - **Order details** – your purchase history (in particular the products or services you have purchased).

	- **Insurance-related information** – information regarding commercial, property or product liability insurance. - **Data collect through our anonymous hotline.** - **Telephone recordings.** - **Content data** uploaded by Avaya customers - **Customer file metadata**
What categories of sensitive personal information (if any) are transferred?	None.
Who are the types of individuals whose personal information are transferred?	Avaya customers and their agents. In this context, a customer means any existing or prospective customer who has entered into a contract or a business relationship with a Avaya entity for the purchase of Avaya products and services. Avaya customers are almost exclusively businesses (in which case Avaya will process data about the customer's agents)..
Why is this personal information transferred and how will it be used?	Avaya may need to transfer the personal information for the following purposes: - to manage account information (management of orders, billing, invoicing, debt collection, etc.); - to fulfil its contractual obligations and to provide its products and services to its customers including on its websites; - to provide information and notifications to its customers regarding the products or services they have purchased or the state and quality of their products; - to provide technical support services to its customers and after sales services (including technical information about our products); - to manage any queries, complaints or claims received from its customers relating to Avaya's products and services; - to provide customized direct marketing, advertising and public relations based on its customers' past activities, and to inform its customers about important developments within Avaya;

	- to manage customer account profiles on its websites and to give access to such profiles. - to comply with applicable laws in terms of product quality and liability, and where necessary to comply with laws and regulations, or to exercise or defend the legal rights of Avaya affiliates; - to help Avaya conduct its business more effectively and efficiently and to check and improve the quality of its products and/or services; - to carry out research and development; - for business development purposes, internal reporting and to conduct analysis and statistical studies about its products and services; - to provide technical education and training to its customers; - to evaluate performance; - to investigate violations of law or breaches of other Avaya's policies, including when reported via Avaya's anonymous hotline.
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.

4. Supply chain management 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 control 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 control described in this section to every Avaya Group Member inside and outside of the EEA.
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 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 inside and outside of the EEA.
What categories of personal information are transferred?	- **Identification data** – name. - **Contact details** – address, telephone, email address, etc. - **Professional details** – job title/position, affiliated organization, office location, etc. - **Financial details** – bank account number, credit worthiness, and credit card details. - **National identifiers** – tax ID and VAT number. - **Order details** –purchase history (in particular the products or services you have purchased). - **Insurance-related information** – information regarding commercial, property or product liability insurance**.** - **Data collect through our anonymous hotline** - **Telephone recordings.**
What categories of sensitive personal information (if any) are transferred?	None
Who are the types of individuals whose personal information are transferred?	Suppliers, vendors, third party service providers and their agents.
Why is this personal information transferred and how will it be used?	Avaya may need to transfer the personal information for the following purposes: - to manage account information (management of orders, billing, invoicing, debt collection, etc.); - to fulfil its contractual obligations and to purchase products and services from it suppliers including on its websites; - to provide information and notifications to its suppliers regarding the products or services they

	have purchased or the state and quality of their products; - to manage supplier account profiles on its systems for payment processing, tracking, etc. - to comply with applicable laws in terms of product quality and liability, and where necessary to comply with laws and regulations, or to exercise or defend the legal rights of Avaya affiliates; - for business development purposes, internal reporting and to conduct analysis and statistical studies about the suppliers' products and services; - to evaluate performance; - to investigate violations of law or breaches of other Avaya's policies, including when reported via Avaya's anonymous hotline.
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.

5. Website visitors' 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 control 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 control described in this section to every Avaya Group Member inside and outside of the EEA.
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 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 inside and outside of the EEA.
What categories of personal information are transferred?	**Identification data** (e.g. name). **Contact details** – address, telephone, email address, etc. **Exchanges between Avaya and a website visitor.** **Personal information collected automatically from the website visitor's computer or mobile device** (“**Device**”), such as: - IP address; - Device type; - unique Device identification numbers; - browser-type; - preferences; - broad geographic location (e.g. country or city-level location); - other technical information; - information about how the device has interacted with Avaya's websites, including the pages accessed and links clicked.
What categories of sensitive personal information (if any) are transferred?	None.
Who are the types of individuals whose personal information are transferred?	Visitors of Avaya's websites.
Why is this personal information transferred and how will it be used?	Avaya may need to transfer this personal information for the following purposes: - to manage the visitor's online accounts; - to manage subscriptions to marketing communications from Avaya and to send Avaya's newsletter or other promotional materials; - to provide customized direct marketing, advertising and public relations based on its visitors' past activities, and to inform its visitors about important developments within Avaya;

	- to respond to a visitor's questions to Avaya; - for internal analytics purposes and to improve the quality and relevance of Avaya's websites to our visitors; - to comply with applicable laws in terms of product quality and liability, and where necessary to comply with laws and regulations, or to exercise or defend the legal rights of Avaya affiliates; - to provide technical education and training to its visitors; - to manage any queries, complaints or claims received from its visitors relating to Avaya products and services; - to process and fulfil orders; - to participate in surveys or - to keep an accurate record of the visitor's information.
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.