Last updated: 11 September 2019

Global Binding Corporate Rules:

Controller and Processor Policies

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 here).

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?

European data protection law prohibits the transfer of personal information to countries outside Europe[3] that do not ensure an adequate level of data protection. Some of the countries in which Avaya operates are not regarded by European 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 Europe and then transferred to a Group Member outside Europe.

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 Europe means the EEA and Switzerland.

- 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**").

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.

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.

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 2.

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 three 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 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 competent data protection authority;
- 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, 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 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 Europe 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 a 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 notify the competent regulator and, where applicable, the individuals affected by the security incident, in accordance with applicable law.

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 1) 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 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 1) in such circumstances.

RULE 8 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

Rule 8 – Avaya will not transfer personal information to third parties outside Europe 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.

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

[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.

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, 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 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 – COMPLAINT HANDLING

Rule 13 – 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 2.

RULE 14 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 14 – 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 3.

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

Rule 15A – Avaya will ensure that where it believes that the legislation applicable to it prevents 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 15B – 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 consult the data protection authority with competent jurisdiction in case of doubt.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under European data protection law, individuals whose personal information is processed in Europe by a Group Member acting as a controller (an "**EEA Entity**") and/or transferred to a Group Member located outside Europe under this Controller Policy (a "**Non-EEA Entity**") have certain rights. Individuals may enforce the principles and rules that are set out in this Controller Policy as third party beneficiaries.

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 2) and may lodge a complaint with a European 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.

If an individual suffers damage, where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Controller Policy, the burden of proof to show that a Non-EEA Entity is not responsible for the breach, or that no such breach took place, will rest with Avaya Deutschland GmbH.

Binding Corporate Rules: Processor Policy

Contents

INTRODUCTION

This Global Binding Corporate Rules: Processor Policy ("**Processor Policy**") establishes Avaya's approach to compliance with data protection law when processing[5] personal information[6] on behalf of and under the instructions of a Controller and specifically with regard to transfers of personal information between members of the Avaya group of entities. This Processor Policy describes how Avaya will comply with data protection law in respect of processing it performs as a processor.

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

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

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

[5] **"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.

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

PART I: BACKGROUND AND SCOPE

WHAT IS DATA PROTECTION LAW?

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

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

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

HOW DOES DATA PROTECTION LAW AFFECT AVAYA INTERNATIONALLY?

European data protection law prohibits the transfer of personal information to countries outside Europe[7] that do not ensure an adequate level of data protection. Some of the countries in which Avaya operates are not regarded by European 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 Processor Policy therefore sets out a framework to satisfy data protection law requirements and in particular, to provide an adequate level of protection for all personal information processed by Avaya globally, either where the personal information is collected by a controller in Europe, or where the personal information is collected by a Group Member in Europe as a processor.

SCOPE OF THIS PROCESSOR POLICY

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

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

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

[7] For the purpose of this Processor Policy reference to Europe means the EEA and Switzerland.

AVAYA'S RESPONSIBILITY TOWARDS A CONTROLLER

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

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

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

LEGALLY BINDING EFFECT OF THIS PROCESSOR POLICY

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

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

FURTHER INFORMATION

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

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

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

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 2.

PART II: PROCESSOR OBLIGATIONS

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

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

Section A addresses the basic principles that Avaya must observe when it processes personal information as a processor.

Section B deals with certain practical data protection commitments made by Avaya in connection with this Processor Policy.

Section C describes the third party beneficiary rights that Avaya grants to individuals in its capacity as a processor under this Processor Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF THE PROCESSING

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

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

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

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

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

Avaya will, without undue delay and as required under the terms of the contract or other legally binding document it has with a Controller, assist that Controller to comply with its obligations under applicable data protection laws. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract or other legally binding document with a Controller, such as providing assistance to that Controller to meet its obligations to keep personal information accurate and up to date.

RULE 2 – FAIRNESS AND TRANSPARENCY

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

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

RULE 3 – PURPOSE LIMITATION

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

Avaya will only process personal information on behalf of the Controller and in compliance with the terms of the contract or other legally binding document with that Controller.

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

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

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

RULE 4 – DATA MINIMIZATION AND ACCURACY

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

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

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

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

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

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

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

RULE 6 – SECURITY AND CONFIDENTIALITY

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

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

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

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

Avaya will notify a Controller of any security breach in relation to personal information processed on behalf of that Controller without undue delay and as required to do so under the terms of the contract or other legally binding document it has with that Controller.

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

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

of the contract or other legally binding document with Avaya and as referred to in Rule 3 of this Processor Policy.

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

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

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

- commitments on the part of the sub-processor regarding the security of that information, consistent with those contained in this Processor Policy and with the terms of the contract or other legally binding document Avaya has with the Controller in respect of the processing in question;

- that the sub-processor will act only on Avaya's instructions when processing that information; and

- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by Avaya in this Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals in respect of transfers of personal information from a Group Member in Europe to a sub-processor established outside Europe.

RULE 7 – RIGHTS OF INDIVIDUALS

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

Avaya will act in accordance with the instructions of a Controller as required under the terms of the contract or other legally binding document with that Controller and undertake any necessary measures to enable a Controller to comply with its duty to respect the rights of individuals. In particular, if Avaya receives a request from an individual to exercise his/her rights, Avaya will transfer such request promptly to the Controller and not respond to such a request unless authorised to do so or required by law. Avaya will follow the steps set out in the Data Subject Rights Procedure (see Appendix 1) when dealing with such requests.

RULE 8 – ACCOUNTABILITY

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

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

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

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

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

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

SECTION B: PRACTICAL COMMITMENTS

RULE 9 – COMPLAINT HANDLING

Rule 9 – 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 2.

Avaya will enable individuals to raise data protection complaints and concerns (including complaints about processing under this Processor Policy) by complying with the Complaint Handling Procedure set out in Appendix 2.

RULE 10 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 10 – Avaya will cooperate with the data protection authorities on any issue related to the Processor Policy in accordance with the Cooperation Procedure set out in Appendix 3.

Avaya will cooperate with the competent data protection authorities by complying with the Cooperation Procedure set out in Appendix 3.

RULE 11 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE PROCESSOR POLICY

Rule 11A – Avaya will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Processor Policy, or such legislation has a substantial effect on its ability to comply with the Processor Policy, Avaya will promptly inform (unless otherwise prohibited by law) the:

- **Controller as provided for by Rule 2 (unless otherwise prohibited by a law enforcement authority);**
- **Data Privacy Officer and the EU entity with data protection responsibilities; or**
- **appropriate data protection authority competent for the Controller and for Avaya.**

Rule 11B – Avaya will ensure that where it receives a legally binding request for disclosure of personal information by a law enforcement authority or state security body which is subject to this Processor Policy, Avaya will:

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

Avaya will use its best efforts to inform the requesting law enforcement authority or state security body about its obligations under European data protection law and to obtain the right to waive this prohibition. Where such prohibition cannot be waived, despite Avaya's efforts, Avaya will provide the competent data protection authorities with an annual report providing general information about any requests for disclosure it may have received from a requesting law enforcement authority or state security body, to the extent that Avaya has been authorized by said authority or agency to disclose such information (in accordance with Appendix 4).

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under European data protection law, individuals whose personal information is processed in Europe by a Group Member acting as a processor (an "**EEA Entity**") and/or transferred to a Group Member located outside Europe under the Processor Policy (a "**Non-EEA Entity**") have certain rights. These individuals may enforce the Processor Policy as third-party beneficiaries where they cannot bring a claim against a Controller in respect of a breach of any of the commitments in this Policy by a Group Member (or by a sub-processor) acting as a processor because:

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

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

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

Complaints: Individuals may complain to an EEA Entity in accordance with the Complaint Handling Procedure (set out in Appendix 2) and may lodge a complaint with a European data protection authority in the jurisdiction of their habitual residence, or place of work, or place of alleged infringement;

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

Compensation:

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

Avaya Deutschland GmbH and where appropriate, receive compensation from Avaya Deutschland GmbH for any material or non-material damage suffered as a result of a breach of this Processor Policy.

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

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

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

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

PART III: APPENDICES

APPENDIX 1

DATA SUBJECT RIGHTS PROCEDURE

1. Introduction

1.1. Avaya's “Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the “**Policies**” or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard personal information transferred between Avaya's Group Members.

1.2. Individuals whose personal information is processed by Avaya under the Policies 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 either as a Controller or a Processor and are transferred under the Policies.

1.4. Where a Request is subject to European data protection law because it is made in respect of personal information processed in Europe, 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:

2.1.1. 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;

2.1.2. 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;

2.1.3. 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;

2.1.4. 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

2.1.5. 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:

3.2.1. where Avaya is the Controller of that individual's personal information under the Controller Policy, it must help the individual to exercise his or her data protection rights directly in accordance with this Procedure; and

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

4. Initial assessment of a Request

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

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

4.2.1. 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

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

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

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

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, 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.

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 Europe 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:

6.2.1.1. the refusal to provide the information or carry out the Access Request of the individual is consistent with the exemptions under current European data protection law;

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

6.2.1.3. the personal information does not originate from Europe, has not been processed by any European 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, either in its capacity as Controller or on instruction of a Controller when it is acting as a processor, Avaya will notify other Group Members or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records, unless this proves impossible or involves disproportionate effort.

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 2

COMPLAINT HANDLING PROCEDURE

1. Background

1.1. Avaya's "Global Binding Corporate Rules: Controller Policy" and "Global Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard personal information transferred between Avaya's group members ("**Group Members**"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal information is processed by Avaya under the Policies are dealt with.

1.2. This procedure will be made available to individuals whose personal information is processed by Avaya under the Controller Policy and, where Avaya processes personal information on behalf of a Controller, to that Controller (under the Processor 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, Building 1000, Cathedral Square, Cathedral Hill, Guildford, Surrey, GU2 7YL, United Kingdom.

3. Complaints where Avaya is a Controller

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 European data protection authority 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 a 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 Europe[8] but then transferred to a Group Member outside Europe and an individual wants to make a claim against Avaya, the claim may be made against the Group Member in Europe responsible for exporting the personal information or the courts of the Member State where the individual has his or her habitual residence.

5. Complaints where Avaya is a processor

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

5.2. Individuals whose personal information is processed in accordance with European data protection law and transferred between Group Members on behalf of a Controller have the right to complain to Avaya and Avaya will handle such complaints in accordance with section 3 of this Complaint Handling Procedure.

5.3. In such cases, individuals also have the right to lodge a complaint with a European data protection authority and to bring proceedings before a court of competent jurisdiction, including when they are not satisfied with the way in which their complaint has been resolved by Avaya. Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

[8] References to Europe for the purposes of this document includes the EEA and Switzerland

APPENDIX 3

COOPERATION PROCEDURE

1. Introduction

1.1. This Global Binding Corporate Rules: Cooperation Procedure sets out the way in which Avaya will cooperate with the European[9] data protection authorities in relation to the "Avaya Global Binding Corporate Rules: Controller Policy" and "Global Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**").

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

2. Material changes to the Policies

2.1. Avaya will communicate any material changes to the Policies (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) without undue delay to the Lead Data Protection Authority and to any other relevant European data protection authorities as appropriate.

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

3. Administrative changes to the Policies

3.1. Avaya will communicate changes to the Policies which:

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

3.1.2. have occurred as a result of either a change of applicable data protection law in any European country or due to any legislative, court or supervisory authority measure,

to the Lead Data Protection Authority and to any other relevant European 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 Policies.

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

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

3.2.2. have occurred as a result of a change of applicable data protection law in any European country or due to any legislative, court or supervisory authority measure,

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

[9] References to Europe for the purposes of this document includes the EEA and Switzerland

4. Communicating changes to the Policies

4.1. Avaya will communicate all changes to the Policies, whether administrative or material in nature:

4.1.1. to the Group Members bound by the Policies via written notice (which may include e-mail); and

4.1.2. systematically to Controllers and individuals who benefit from the Policies via www.avaya.com.

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

5. Logging changes to the Policies

5.1. The Policies contain a change log which sets out the date each 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 Policies.

5.2. Avaya will also maintain an accurate and up-to-date list of all Group Members that are bound by the Policies. 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 Policies before a transfer of personal information to them takes place.

APPENDIX 4

LAW ENFORCEMENT DATA ACCESS PROCEDURE

1. Introduction

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

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

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

2. General principle on Data Production Requests

2.1. As a general principle, Avaya does not disclose personal information in response to a Data Production Request unless either:

2.2. it is under a compelling legal obligation to make such disclosure; or

2.3. taking into account the circumstances and the privacy rights of any affected individuals, there is an imminent risk of serious harm for the data subject or another natural person that merits disclosure in any event.

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

2.5. For that reason, unless it is legally compelled to do so or there is an imminent risk of serious harm for the data subject or another natural person, Avaya will first consult with the competent data protection authorities and provide the Controller with details of the Data Production Request. Avaya will cooperate with the competent data protection authorities and the Controller to address the Data Production Request.

3. Data Production Request review

3.1. Receipt of a Data Production Request

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

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

3.2. Initial steps

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

laws and to identify whether action may be needed to challenge the Data Production Request.

4. Notice of a Data Production Request

4.1. Notice to the Controller

4.1.1. After assessing the nature, urgency, scope and validity of the Data Production Request, Avaya will notify and provide the Controller with the details of the Data Production Request prior to disclosing any personal information, unless legally prohibited or where the imminent risk of serious harm for the data subject or another natural person prohibits prior notification.

4.2. Notice to the competent data protection authorities

4.2.1. Avaya will also put the request on hold in order to notify and consult with the competent data protection authorities, unless legally prohibited or where the imminent risk of serious harm for the data subject or another natural person prohibits prior notification.

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

5. Transparency reports

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

6. Queries

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