Zendesk

EU Binding Corporate Rules

Controller Policy

Contents

Part I: Introduction

This Binding Corporate Rules: Controller Policy (“Controller Policy”) establishes Zendesk's approach to compliance with European data protection law and specifically to transfers of personal data between Zendesk group members ("Group Members" or “Zendesk”) (a list of which is available at Appendix 1: List of Group Members).

Scope of this Controller Policy

This Controller Policy applies to all personal data processed by Zendesk as a controller whenever it is collected and used by Zendesk Group Members or as an internal processor on behalf of another Group Member acting as a controller. This Controller Policy applies regardless of whether our Group Members process personal data by manual or automated means.

For an explanation of some of the terms used in this Controller Policy, like "controller", "process", "personal data", and "personal data breach", please see the section entitled "Important terms used in this Controller Policy” below.

Group Members process personal data for Zendesk business activities (such as, products and services management, analysis and monitoring, marketing activities, customer support, training and other individualized services we provide our customers), employment administration (including, but not limited to, carry out HR management, payroll, training, recruitment, performance evaluations and analysis, health and safety processing, reporting, physical, network and devices security, strategic projects and transactions, and other HR processing) and vendor management (such as, supply/services and business continuity management). As such, the personal data to which this Policy applies includes:

- CRM and other business management data about Zendesk's current, former and prospective customers (and their representatives), including but not limited to personal, contact and financial details, marketing preferences and other personal data exchanged in the course of regular business.
- human resources data about Zendesk staff members, including but not limited to, employment and evaluations records, identifiers, salary and training details, qualifications, benefits and other HR management-related information, and
- vendor data about Zendesk 's current, former and prospective suppliers and service providers (and their representatives), including, but not limited to contact details, financial details, customer (company) details, and other business related information.

The personal data may be processed in every territory where Group Members or our processors are located.

Our collective responsibility to comply with this Controller Policy

All Group Members and their staff will comply with, and respect, this Controller Policy when processing personal data as a controller, irrespective of the country in which they are located.

In particular, all Group Members who process personal data as a controller will comply with:

- the rules set out in Part II of this Controller Policy;
- the practical commitments set out in Part III of this Controller Policy;
- the third party beneficiary rights set out in Part IV of this Controller Policy; and
- the policies and procedures appended in Part V of this Controller Policy.

Management commitment and consequences of non-compliance

Zendesk's management is fully committed to ensuring that all Group Members and their staff comply with this Controller Policy.

Non-compliance may cause Zendesk to be subject to sanctions imposed by competent data protection authorities and courts and may cause harm or distress to individuals whose personal data has not been protected in accordance with the standards described in this Controller Policy.

In recognition of the gravity of these risks, staff members who do not comply with this Controller Policy may be subject to disciplinary or other appropriate action, up to and including dismissal, subject to applicable labour and employment laws and internal Zendesk policies.

Relationship with Zendesk's Binding Corporate Rules: Processor Policy

This Controller Policy applies only to personal data that Zendesk processes as a controller.

Zendesk has a separate Binding Corporate Rules: Processor Policy that applies when it processes personal data as a processor in order to provide a service to a third party (such as a customer) or as an internal processor on behalf of another Group Member acting as a controller. When a Zendesk Group Member processes personal data as a processor, it will comply with the Processor Policy.

In some situations, Group Members may act as both a controller and an internal processor. Where it acts as a processor on behalf of an external controller to provide a service to Zendesk, Group Members will comply both with this Controller Policy and the Processor Policy.

Where will this Controller Policy be made available?

This Controller Policy will be published on the Zendesk website accessible at www.zendesk.com, containing all elements listed in this Controller Policy.

Important terms used in this Controller Policy

For the purposes of this Controller Policy and to the extent it applies:

- the term *applicable data protection laws* includes the data protection laws applicable to respective Group Members processing of personal data at the time of such processing. Where a European Group Member transfers personal data under this Controller Policy, the term applicable data protection laws shall mean the European data protection laws applicable to that controller;
- the term *applicable law* includes European laws, rules and regulations applicable to respective Group Members or those extra-territorial laws, rules and regulations applicable to Group Members related to their activities under this Controller Policy;
- the term *competent data protection authority* means the European data protection (supervisory) authority competent for the data exporter;
- the term *controller* means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- the term *Controller Policy* refers to these Binding Corporate Rules: Controller Policy, which is available at www.zendesk.com. The Controller Policy applies where Zendesk processes personal data as a controller (i.e. for its own purposes);
- the term *customer* refers to the third-party controller or processor on whose behalf Zendesk processes personal data. This includes Zendesk's third-party customers, when Zendesk processes personal data on their behalf in the course of providing services to them;
- the term *data exporter* means a Group Member that transfers personal data which is subject to European data protection laws to another Group Member outside of Europe;
- the term *data importer* means a Group Member that receives personal data from the data exporter;
- the term Europe (and European) as used in this Controller Policy refers to the European Economic Area and its Member States – that is, the Member States of the European Union plus Norway, Lichtenstein and Iceland;
- the term *personal data* means any information relating to an identified or identifiable natural person. 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;

- the term *personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by Zendesk or its processors or sub-processors;
- the term *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;
- the term *processor* means a natural or legal person which processes personal data on behalf of a controller (for example, a third-party service provider that is processing personal data in order to provide services to Zendesk);
- Binding Corporate Rules: Processor Policy means Zendesk's Binding Corporate Rules: Processor Policy, which applies where Zendesk processes personal data as a processor on behalf of a third party;
- the term *sensitive personal data* means information that relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation; and
- the term *staff* refers to all employees, temporary staff or equivalent positions in Zendesk engaged by any Zendesk Group Member.

How to raise questions or concerns

If you have any questions regarding this Controller Policy, your rights under this Controller Policy or applicable data protection laws, or any other data protection issues, you can contact the Chief Privacy Officer at the address below. Zendesk's Chief Privacy Officer will either deal with the matter in consultation with the Zendesk Privacy Council or forward it to the appropriate person or department within Zendesk.

Attention: Chief Privacy Officer Email: privacy@zendesk.com Address: 181 S. Fremont St. San Francisco, California 94105 United States

The Zendesk Privacy Council is responsible for ensuring that changes to this Controller Policy are notified, without undue delay, to the Group Members and to individuals whose personal data is processed by Zendesk in accordance with Appendix 8.

If you want to exercise any of your data protection rights, please see the data protection rights procedure set out in Appendix 2. Alternatively, if you are unhappy about the way in which Zendesk has used your personal data, Zendesk has a separate complaint handling procedure which is set out in Appendix 6.

Part II: Zendesk's obligations

This Controller Policy applies in all situations where a Group Member collects, uses and transfers personal data as a controller. All staff and Group Members will comply with the following obligations:

Rule 1 – Lawfulness: Zendesk will be compliant with applicable data protection law and this Controller Policy.	Zendesk will comply with applicable data protection laws, as well as standards set out in this Controller Policy, when processing personal data. As such: ● where applicable data protection laws exceed the level of protection of personal data set out in this Controller Policy, Zendesk will comply with those laws; but ● where there are no applicable data protection laws, or where applicable data protection laws do not meet the standards set out by this Controller Policy, Zendesk will process personal data in accordance with this Controller Policy.

	Zendesk will ensure it has a lawful basis for processing personal data, consistent with the requirements of applicable data protection laws. Zendesk will process personal data processed subject to the Controller Policy in line with Appendix 13.
Rule 2 – Fairness and transparency: Zendesk will explain to individuals, at the time their personal data is collected, how their information will be used.	Zendesk will provide individuals with the Fair Information Disclosures in line with Appendix 12. Zendesk will take appropriate measures to communicate the Fair Information Disclosures to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Fair Information Disclosures shall be provided in writing, or by other means, including, where appropriate, by electronic means. They may be provided orally, at the request of an individual, provided that the identity of that individual is proven by other means. Zendesk will explain how their personal data will be used (usually by means of an easily accessible privacy notice or privacy statement). This information will be provided when personal data is obtained by Zendesk from the individual or, if not practicable to do so at the point of collection, as soon as possible after collection when data has been obtained from third parties, from a publicly available source, and not directly from the data subject. In limited cases, Zendesk may not need to provide the Fair Information Disclosures (for example, because the individual already has the information, the provision of the Fair Information Disclosures may prove impossible or involve a disproportionate effort, or where otherwise permitted by law). Where this is the case, Zendesk will decide what course of action is appropriate to protect

	the individual's rights, freedoms and legitimate interests. Zendesk will follow this Rule 2 unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, legal proceedings, or where otherwise permitted by law).
Rule 3 – Purpose limitation: Zendesk will process personal data only for specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those purposes.	Where Zendesk collects personal data in the Europe and where local law requires that Zendesk only process personal data for specified, explicit and legitimate purposes determined at the time of collection and that have been communicated to the individuals concerned in accordance with Rule 12. Zendesk will not process the personal data in a way that is incompatible for those purposes, except in accordance with applicable law. If Zendesk intends to process personal data for a purpose which is incompatible with the purpose for which the personal data was originally collected, Zendesk may only do so if such processing is permitted by lawful basis. Zendesk will also provide the individual with Fair Information Disclosures about the further processing in accordance with Rule 12.
Rule 4 – Data minimization: Zendesk will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.	Zendesk will only process personal data that is adequate, relevant and limited in order to properly fulfil the desired processing purposes. Zendesk will not process personal data that is unnecessary to achieve those purposes.
Rule 5 – Data accuracy: Zendesk will keep personal data accurate and, where necessary, up to date.	Zendesk will take reasonable measures to confirm that the information Zendesk processes is accurate and, where necessary, kept up to date – for example, by

	actively encouraging individuals to inform Zendesk when their personal data has changed or has otherwise become inaccurate. Zendesk will take every reasonable step to confirm that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Rule 6 – Storage limitation: Zendesk will only keep personal data for as long as is necessary for the purposes for which it is collected and further processed.	Zendesk will not keep personal data in a form which permits identification of individuals for longer than is necessary for the purposes for which the personal data is processed, unless there is a legal ground for further processing. In particular, Zendesk will comply with Zendesk's record retention policies and guidelines as revised and updated from time to time.
Rule 7 – Security, integrity and confidentiality: Zendesk will implement appropriate technical and organizational measures.	Zendesk will implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of personal data over a network, and against all other lawful forms of processing. Such measures will take account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. To this end, Zendesk will comply with the requirements in the security policies in place within Zendesk, as revised and updated from time to time, together with any other security procedures relevant to a business area or function.

	Zendesk will limit access to personal data to authorized individuals, who will only process personal data on instructions from the relevant Group Member. Such Zendesk staff members are under a duty of confidentiality.
Rule 8 – Service provider management: Zendesk will ensure that service providers will utilize appropriate and equivalent security measures when processing personal data.	Where a Group Member appoints a service provider to process personal data on its behalf (i.e. a processor), Zendesk will impose strict contractual terms, in writing, ensuring that service provider will: ● act only in accordance with Zendesk's documented instructions when processing that personal data, including with regard to international transfers of personal data and onward transfers to a third country unless required to do so by applicable data protection law to which the service provider is subject; in such a case, the service provider shall inform Zendesk of this requirement if it is no longer able to process personal data in accordance with applicable data protection law, unless that law prohibits such information on important grounds of public interest; ● to confirm a duty of confidentiality or any appropriate statutory obligation of confidentiality of any individuals who have access to or otherwise process the personal data subject to this Controller Policy; ● have in place appropriate technical and organizational security measures to ensure a level of security appropriate to the risk to safeguard the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Such measures will take account the state of the art, the costs of implementation and the

	nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons; ● only engage a sub-processor if Zendesk has given its prior specific or general written authorization, and on condition that (i) the sub-processor agreement protects the personal data to substantially the same standard required of the service provider, in particular, the sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of applicable data protection law; and (ii) the service provider remains liable to Zendesk for the performance of the sub-processor's data protection obligations; ● taking into account the nature of the processing and the information available to the service provider, assist Zendesk in ensuring compliance with its obligations as a controller under applicable data protection laws, in particular with respect to (i) reporting personal data breaches under Rule 9, (ii) security obligations meeting or exceeding those defined by applicable data protection laws; (iii) data protection impact assessments under Rule 15, and (iv) assisting Zendesk with any prior consultations required as a result of a data protection impact assessment; ● taking into account the nature of the processing, the processor (or its sub-processor, as applicable) assists Zendesk by appropriate technical and organisational measures, insofar as this is possible,

	for the fulfilment of Zendesk's obligation to respond to requests for exercising the data subject's rights; ● return or delete the personal data once it has completed its services and deletes existing copies, unless law requires storage of the personal data, in line with applicable data protection laws; and ● make available to Zendesk all necessary information in order to demonstrate its compliance with these obligations and allow for and contribute to audits, including inspections. conducted by Zendesk or another auditor mandated by Zendesk.
Rule 9 – Personal data breach reporting: Zendesk will comply with any personal data breach reporting requirements that exist under applicable data protection law.	In the event a member of Zendesk staff becomes aware of a personal data breach, Zendesk staff will notify the Information Security team. The Information Security team will review the nature and seriousness of the personal data breach with the privacy team. The privacy team shall be responsible for ensuring that any notifications to the data protection authority or data subjects, where necessary, are made in accordance with the requirements of applicable data protection law. The privacy team will notify personal data breaches of personal data processed subject to this Controller Policy in line with Appendix 10.
Rule 10 – Data protection rights: Zendesk will enable individuals to exercise their data protection rights in accordance with applicable data protection law.	● In accordance with Appendix 2, Zendesk will honour the following data protection rights: right of access, notification regarding rectification or erasure or restriction, restriction of processing, data portability, object to the processing, and to not be subject to automated individual decision making. ● Where an individual wishes to exercise any of its data protection rights, Zendesk will respect those

	rights in accordance with applicable data protection law by following the Data Protection Rights Procedure (see Appendix 2).
Rule 11 – Adequate protection for international transfers: Zendesk will not transfer internationally without ensuring appropriate safeguards for the information in accordance with the standards set out by this Policy.	Applicable data protection laws may prohibit international transfers of personal data to third countries, unless appropriate safeguards are implemented. This includes transfers of personal data from Group Members to third parties who are not subject to this Controller Policy. Group Members will not transfer personal data to other non-European Group Members subject to this Controller Policy until they are effectively bound by it and can deliver compliance with it (including privacy training as outlined in Part III of this Controller Policy). When transferring personal data internationally, or onward transferring personal data to third parties, Zendesk will be consulted so that they can confirm appropriate safeguards. When (onward) transferring of personal data processed subject to the Controller Policy, to controller or processor recipients not bound by the Controller Policy, Zendesk will ensure that one of the following applies: ● recipients are in a third country which the European Commission recognized as providing an adequate level of protection to personal data; ● transfer is subject to appropriate safeguards provided in applicable data protection law (including binding corporate rules; standard or other competent data protection authority-authorized data protection clauses; approved codes of conduct; and certification mechanisms); or

	● in the absence of the above two options, transfer is subject to derogations for specific situations provided in applicable data protection law (including individual's explicit consent; necessity to conclude/perform a contract with or in the interest of the individual; transfer is necessary for important public interests, establishment, exercise or defence of legal claims, or to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent). The transfer can otherwise only take place if competent supervisory authority has been informed and it is not repetitive, concerns only a limited number of individuals, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the individual, and the controller has assessed and provided suitable data protection safeguards.
Rule 12 – Sensitive personal data: Zendesk will only process sensitive personal data collected in Europe where the individual's explicit consent has been obtained, unless Zendesk has an alternative legitimate basis for processing consistent with applicable data protection law.	Zendesk will assess whether sensitive personal data is required for the intended purposes before collecting it or otherwise processing. Before processing sensitive personal data, Zendesk will obtain the individual's explicit consent or will have another lawful basis consistent with the applicable data protection laws. Zendesk will process sensitive personal data processed subject to this Controller Policy in line with Appendix 13.
Rule 13 – Direct Marketing: Zendesk will allow all individuals to opt-out of receiving marketing information.	All individuals have the right to object, free of charge and at any time, to the use of their personal data for

	direct marketing purposes. Zendesk will honour all such opt-out requests.
Rule 14 – Automated individual decision-making, including profiling: Zendesk will respect individuals' rights not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.	Under applicable data protection law, no decision, which produces legal effects concerning an individual, or similarly significantly affects that individual, can be based solely on the automated processing of that individual's personal data, including profiling, unless such decision is: ● necessary for entering into, or performing, a contract between a Group Member and that individual; ● authorized by applicable data protection law (which in the case of personal data about European individuals, must be European law); or ● based on the individual's explicit consent. In the first and third cases above, Zendesk will implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express his or her view and to contest the decision. Zendesk will not make automated individual decisions about individuals using their sensitive personal data unless they have given explicit consent under Rule 12 or another lawful basis applies.
Rule 15 – Data Protection Impact Assessments: Zendesk will carry out data protection impact assessments where processing is likely to result in a high risk to rights and freedoms of individuals and consult, where	Where required by applicable data protection laws, Zendesk will carry out data protection impact assessments ("DPIAs") whenever the processing of personal data, particularly using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high

required by law, with competent data protection authorities.	risk to the rights and freedoms of individuals. This includes, in particular: ● automated processing-based (including profiling) systematic and extensive evaluation of personal aspects relating to natural persons on which decisions with significant effects on individuals are based; ● large-scale processing of sensitive personal data or of personal data relating to criminal convictions and offences; and ● large-scale systematic monitoring of a publicly accessible area. Zendesk will carry out a DPIA prior to processing which will contain at least the following: ● A systematic description of the envisaged processing operations and the purposes of the processing; ● An assessment of the necessity and proportionality of the processing operations in relation to the purposes; ● An assessment of the risks to the privacy rights and freedoms of individuals; and ● The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with applicable data protection laws. Where the DPIA indicates that the processing would still result in a high risk to individuals, Zendesk will consult with competent data protection authorities where required by applicable data protection laws and

	provide them with relevant information regarding the intended processing and other relevant information. Zendesk monitors, on an ongoing basis, and where appropriate in collaboration with processors and other Group Members acting as data importers, developments in the third countries to which processors and Group Members acting as the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.
Rule 16 – Data protection by design and by default: Zendesk will apply data protection by design and by default when designing and implementing new products and systems.	When designing and implementing new products and systems which process personal data, Zendesk will take into account the state of the art, cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, implement data protection by design and by default, where required by applicable data protection laws. This means implementing appropriate technical and organizational measures that: ● are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of individuals and meet the requirements of applicable data protection laws ("privacy by design"); and ● confirm that, by default, personal data is not made accessible to an indefinite number of people without the individual's intervention ("privacy by default").

Part III: Delivering compliance in practice

To ensure Zendesk follows the rules set out in this Controller Policy, in particular the obligations set out in Part II, Zendesk and all of its Group Members will also comply with the following practical commitments:

Resourcing and Compliance: Zendesk will have appropriate staff and support to oversee privacy compliance throughout the business.	Zendesk has appointed its Chief Privacy Officer to oversee and confirm compliance with this Controller Policy. The Chief Privacy Officer is supported by the Zendesk Privacy Council, who is responsible for overseeing and enabling day-to-day compliance with this Controller Policy at a regional and compliance level. Privacy Council is further supported by members, who staff the broader privacy team, including members of the Privacy Council, legal and other internal departments. Zendesk has appointed a group Data Protection Officer ("DPO"). A summary of the roles and responsibilities of Zendesk's privacy team and the DPO is set out in Appendix 3.
Privacy Training: Zendesk will ensure staff are educated about the need to protect personal data in accordance with this Controller Policy.	Group Members will provide appropriate, up-to-date training to staff who: ● have permanent or regular access to personal data; or ● who are involved in the processing of personal data or in the development of tools used to process personal data. Zendesk will provide such training in accordance with the training requirements attached as Appendix 4.
Records of Data Processing: Zendesk will maintain records of the data processing activities under its responsibility	Zendesk will maintain a record of the processing activities that it conducts in accordance with applicable data protection laws, containing information outlined in Appendix 11. These records will be kept in writing

as required by applicable data protection laws.	(which may mean in electronic form) and Zendesk will make these records available to competent data protection authorities upon request. The Chief Privacy Officer is responsible for ensuring that such records are maintained.
Audit: Zendesk will have data protection audits on a regular basis.	Zendesk will have data protection audits on a regular basis, which may be conducted by either internal or external accredited auditors. In addition, Zendesk will conduct data protection audits on specific request from the Privacy Council. Zendesk will conduct any such audits in accordance with the Audit Protocol set out in Appendix 5.
Complaint handling: Zendesk will enable individuals to raise data protection complaints and concerns.	Group Members will enable individuals to raise data protection complaints and concerns (including complaints about processing under this Controller Policy) by complying with the Complaint Handling Procedure (see Appendix 6). Group Members accept that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.
Cooperation with competent data protection authorities: Zendesk will always cooperate with competent data protection authorities.	Group Members will cooperate with competent data protection authorities by complying with the Cooperation Procedure (see Appendix 7).
Updates to this Controller Policy: Zendesk will update this Controller Policy in accordance with its Updating Procedure.	Whenever updating this Controller Policy Zendesk will comply with the Updating Procedure set out in Appendix 8.
Conflicts between this Controller Policy and national legislation:	If applicable data protection laws prevent any Group Member from fulfilling its obligations under this Controller Policy or otherwise is likely to have a

Zendesk will take care where local laws conflict with this Controller Policy, and act responsibly to confirm a high standard or protection for the personal data in such circumstances.	substantial adverse effect on the guarantees provided by this Controller Policy, the Group Member will promptly inform the Chief Privacy Officer, unless otherwise prohibited by law. Where there is a conflict between the legislation applicable to Zendesk and this Controller Policy, the Chief Privacy Officer will make a responsible decision on the action to take and will report, without undue delay, to the competent data protection authority, where conflict is likely to have a substantial adverse effect on the guarantees provided by this Controller Policy, unless otherwise prohibited by law, in which case, Zendesk will use its best efforts to waive this prohibition in order to communicate as much information as it can and as soon as possible, and document such efforts, and otherwise report/provide information about such instances in accordance with Appendix 7.
Government requests for disclosure of personal data:	If a Group Member receives a legally binding request for disclosure of personal data subject to this Controller Policy, by a law enforcement or government authority or state security body, it will comply with the Government Data Request Procedure set out in Appendix 9.
General commitment to the responsibilities in this Controller Policy and responsibilities when there is an inability to comply with this Controller Policy:	No transfer is made to a Group Member unless the Group Member is effectively bound by this Controller Policy and can deliver compliance. A Group Member is required to promptly inform the data exporter if it is unable to comply with the Controller Policy, for whatever reason, including the situations further described throughout this Controller Policy.

	If a Group Member, acting as a data importer, is in breach of this Controller Policy or is unable to comply with them, the data exporter should suspend the transfer. The Group Member, acting as a data importer should, at the choice of the data exporter, immediately return or delete the personal data that has been transferred under the Controller Policy in its entirety, where: ● the data exporter has suspended the transfer, and compliance with this Controller Policy is not restored within a reasonable time, and in any event within one month of suspension; or ● the data importer is in substantial or persistent breach of this Controller Policy; or ● the data importer fails to comply with a binding decision of a competent court or competent data protection authority regarding its obligations under this Controller Policy. The same commitments apply to any copies of personal data. The data importer should certify the deletion of the data to the data exporter. The data importer shall ensure continued compliance with this Controller Policy until such personal data is returned/deleted, including where local applicable laws prohibit return/deletion, and not process personal data beyond what is required by such laws.
Continued protection after termination:	If such data importer agrees with relevant data exporter(s) on retaining personal data it received under this Controller Policy, they must put in place other safeguards in accordance with Rule 11 (Adequate protection for international transfers) above.

Part IV: Third party beneficiary rights

Application of this Part IV

This Part IV applies where individuals' personal data are protected under applicable data protection laws (including the General Data Protection Regulation). This is the case when:

- those individuals' personal data are processed in the context of the activities of a Group Member (or its third party processor) established in Europe;
- a non-European Customer (acting as controller) or Group Member (or its third-party processor) offers goods and services (including free goods and services) to those individuals in Europe; or
- a non-European Customer (acting as controller) or Group Member (or its third-party processor) monitors the behaviour of those individuals, as far as their behaviour takes place in Europe;

and that Group Member then transfers those individuals' personal data to a non-European Group Member for processing under this Controller Policy.

Zendesk will inform all such individuals about their third party beneficiary rights and about the means to exercise them by publishing these in accordance with Part I of this Controller Policy (see: Where will this Controller Policy be made available?).

Entitlement to effective remedies

When this Part IV applies, individuals have the right to pursue effective remedies in the event their personal data is processed by Zendesk in breach of the following provisions of this Controller Policy:

- Part II (Zendesk's Obligations) of this Controller Policy;
- Paragraphs 5 (Complaints Handling), 6 (Cooperation with Data Protection Authorities), 8 (Conflicts between this Policy and national legislation) and 9 (Government requests for disclosure of personal data) under Part III of this Controller Policy; and
- Part IV (Third Party Beneficiary Rights) of this Controller Policy.

Individuals' third party beneficiary rights

When this Part IV of this Controller Policy applies, individuals may exercise the following rights:

- Complaints: Individuals may complain to a Group Member and/or to a competent data protection authority, in accordance with the Complaints Handling Procedure at Appendix 6;

- Proceedings: Individuals may commence proceedings against a Group Member for violations of this Controller Policy, in accordance the Complaints Handling Procedure at Appendix 6;
- 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 Zendesk for the damage suffered as determined by a court of competent jurisdiction in accordance the Complaints Handling Procedure at Appendix 6;
- Transparency: Individuals also have the right to be informed, without undue delay, of all changes to the Policies and to the list of Group Members bound by the Policies, and to obtain a copy of this Controller Policy on request at privacy@zendesk.com.
- Representation: The Group Members accept that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

Responsibility for breaches by non-European Group Members

Zendesk International Ltd. will be responsible for ensuring that any action necessary is taken to remedy any breach of this Controller Policy by a non-European Group Member.

In particular:

- If an individual can demonstrate damage it has suffered likely occurred because of a breach of this Controller Policy, Zendesk International Ltd. will have the burden of proof to show that the non-European Group Member is not responsible for the breach, or that no such breach took place.
- Where a non-European Group Member fails to comply with this Controller Policy, individuals may exercise their rights and remedies above against Zendesk International Ltd. and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Zendesk International Ltd. for any material or non-material damage suffered as a result of a breach of this Controller Policy, as if the breach had been caused by Zendesk International Ltd. in Ireland.

Shared liability for breaches with processors

Where Zendesk has engaged a third-party processor to conduct processing on its behalf, and both are responsible for harm caused to an individual by processing in breach of this Controller Policy, Zendesk accepts that both Zendesk and the processor may be held liable for the entire damage in order to provide effective compensation of the individual.

Part V: Appendices

Appendix 1: List of Group Members

Name of entity	Registered address	Registration number
Zoro TopCo, LP	1209 Orange Street, Wilmington, DE 19801, United States	7122933
Zendesk, Inc.	181 S. Fremont St., San Francisco, CA 94105, United States	4661237
Zendesk UK Limited	30 Eastbourne Terrace, London, W2 6LA, United Kingdom	07622459
Zendesk Technologies Spain S.L.	Paseo de la Castellana, 35 - 5ª planta 28046 Madrid, Spain	Q24PN74
Zendesk Technologies Private Limited	Zendesk Technologies Pvt. Limited, WeWork Galaxy #43, Residency Road, Srinivas Nagar, Shanthala Nagar, Ashok Nagar, Bangalore 560 025, India	U72200KA2016FTC093304
Zendesk Sweden AB	Bolagsratt Sundsvall AB, Box 270, 851 04 Sundsvall, Stockholm, Sweden	559369-0356
Zendesk Singapore Pte. Ltd.	9 Straits View #9-08, Marina One West Tower, Singapore	201009107C

Name of entity	Registered address	Registration number
Zendesk S. de R.L. de C.V.	Avenida Presidente Masaryk 111, 1st floor, Polanco V Sección, Miguel Hidalgo, zip 11560, Mexico City, Mexico	N-201703194
Zendesk Pty., Ltd	3/395 Collins Street, Melbourne, VIC 3000 Australia	151 424 770
Zendesk Netherlands B.V	Strawinskylaan 4117, 1077ZX Amsterdam	864472390
Zendesk Korea LLC	WeWork Gangnam Station, 373 Gangnam-daero Seocho-gu, South Korea	110115-0007175
Zendesk Italy S.r.l.	Via Giuseppe Mazzini 9 Milano, Milano, 20213 Italy	12662030969
Zendesk International Limited	55 Charlemont Place, St. Kevins, Dublin, D02 F985, Ireland	519184
Zendesk Incorporated	30th floor, Seven/NEO 5th Ave., E-Square, Crescent Park West, The Fort, Taguig City, Metro Manila, 1634 Fort Bonifacio, Philippines	CS201400321

Name of entity	Registered address	Registration number
Zendesk GmbH	Zendesk GmbH, c/o WeWork, Neue Schönhauser Straße 3 – 5, Germany	HRB 166170 B
Zendesk France SAS	266 place Ernest Granier, Ark Jacques Coeur 34000 Montpellier, France	513568330 00040
Zendesk Brasil Software Corporativo Ltda	Av Paulista, 854, Andar 10 Sala 1.010, Bela Vista, Sao Paulo SP, CEP 01310-913 Brazil	CNPJ No: 19.722.152/0001-26
Zendesk APS	Snaregade 12, 2nd & 3rd floor DK-1205 København K Denmark	30801830
ZD Sub Holdings	3500 South Dupont Highway, Dover, DE 19901, United States	5420319
Tymeshift doo Novi Sad	Bulevar Oslobodjenja 83, Novi Sad 21000, Serbia	21551945
Smooch Technologies US Inc.	Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801, United States	6023662

Name of entity	Registered address	Registration number
Smooch Technologies ULC	1600 - 925 West Georgia Street, Vancouver, British Columbia V6C 3L2, Canada	BC1208247
OÜ Qualitista	Vana-Lõuna tn 39/1-1, 10134 Tallinn, Estonia	14308859
Kabushiki Kaisha Zendesk	2-1, Kyobashi 2-chome, Chuo-ku ,20th Floor Unit: 2001-4 Tokyo, Japan, 104-0031	0104-01-104446
FutureSimple Inc.	Corporation Trust Center, 1209 Orange Street, Wilmington, County of New Castle, 19801, United States	Delaware: 4659947
Cleverly, Unipessoal, LDA	Avenida da Liberdade, 249, 8º, 1250-143, Lisbon, Portugal	515 089 320
Base sp. z o. o. (Base spółka z ograniczoną odpowiedzialnością)	Wyczółkowskiego 7, 30-118 Kraków, Poland	0000433377

APPENDIX 2: DATA PROTECTION RIGHTS PROCEDURE

1. Introduction

1.1 Zendesk'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 data transferred between the Zendesk Group Members.

1.2 Individuals whose personal data is processed by Zendesk under the Policies have certain data protection rights, which they may exercise by making a request to the controller of their information (whether the controller is Zendesk or a Customer) (a “Data Protection Rights Request”).

1.3 This Binding Corporate Rules: Data Protection Rights Procedure (“Procedure”) describes how Zendesk will respond to any Data Protection Rights Request it receives from individuals whose personal data is processed and transferred under the Policies.

1.4 Where a Data Protection Rights Request is subject to applicable data protection law because it is made in respect of personal data collected and/or used in Europe, such request will be dealt with by Zendesk in accordance with this Procedure, but where the applicable data protection law requires a higher level of protection for personal data than this Procedure, the applicable data protection law will prevail.

2. Individuals' data protection rights

2.1 Zendesk will assist individuals to exercise the following data protection rights, consistent with the requirements of applicable data protection laws:

2.1.1 The right to access: This is a right for individuals to obtain confirmation whether a controller processes personal data about them and, if so, to be provided with access to, and a copy of, that personal data. The process for handling this type of request is described further in paragraph 4 below.

2.2.2 The right to rectification: This is a right for individuals to require a controller to rectify without undue delay any inaccurate personal data a controller may process about them. The process for handling this type of request is described further in paragraph 5 below.

2.2.3 The right to erasure: This is a right for individuals to require a controller to erase personal data about them on certain grounds – for example, where the personal data is no longer necessary to fulfil the purposes for which it was collected. The process for handling this type of request is described further in paragraph 5 below.

2.2.4 The right to restriction: This is a right for individuals to require a controller to restrict processing of personal data about them on certain grounds. The process for handling this type of request is described further in paragraph 5 below.

2.2.5 The right to object: This is a right for individuals to object, on grounds relating to their particular situation, to a controller's processing of personal data about them, if certain grounds apply. The process for handling this type of request is described further in paragraph 5 below.

2.2.6 The right to data portability: This is a right for individuals to receive personal data concerning them from a controller in a structured, commonly used and machine readable format and to transmit that data to another controller, if certain grounds apply. The process for handling this type of request is described further in paragraph 6 below.

3. Responsibility to respond to a Data Protection Rights Request

3.1 Overview

3.1.1 The controller of an individual's personal data is primarily responsible for responding to a Data Protection Rights Request and for helping the individual concerned to exercise rights under applicable data protection laws.

3.1.2 An individual contacts Zendesk to make any Data Protection Rights Request then:

(a) where Zendesk is the controller of that individual's personal data under the Controller Policy, Zendesk will help the individual to exercise such data protection rights directly in accordance with this Procedure; and

(b) where Zendesk processes that individual's personal data as a processor on behalf of a Customer under the Processor Policy,

Zendesk will promptly direct the individual to Customer/controller and provide Customer with reasonable assistance to help the individual to exercise such rights in accordance with the Customer's duties under applicable data protection laws.

3.2 Assessing responsibility to respond to a Data Protection Rights Request.

3.2.1 If a Group Member receives a Data Protection Rights Request from an individual, it will pass the request to privacy@zendesk.com promptly upon receipt indicating the date on which it was received the request together with any other information which may assist Zendesk privacy team to respond to the request.

3.2.2 The Zendesk privacy team will make an initial assessment of the request as follows:

(a) the Zendesk privacy team will determine whether Zendesk is a controller or processor of the personal data that is the subject of the request;

(b) where Zendesk privacy team, determines that Zendesk is a controller of the personal data, Zendesk will then determine whether the request has been made validly under applicable data protection laws (in accordance with section 3.3 below), whether an exemption applies (in accordance with section 3.4 below), and respond to the request (in accordance with section 3.5 below); and

(c) where Zendesk privacy team determines that Zendesk is a processor of the personal data on behalf of a Customer, it will promptly direct the individual to the Customer in accordance with its contract terms with that Customer and will not respond to the request directly unless authorised to do so by the Customer under its contract with Zendesk.

3.3 Assessing the validity of a Data Protection Rights Request.

3.3.1 If the Zendesk privacy team determines that Zendesk is the controller of the personal data that is the subject of the request, it will contact the individual promptly in writing to confirm receipt of the Data Protection Rights Request.

3.3.2 A Data Protection Rights Request must generally be made in writing, which can include email, unless applicable data protection laws allow a request to be made orally. A Data Protection Rights Request does not have to be official or mention data protection law to qualify as a valid request.

3.3.3 If Zendesk has reasonable doubts concerning the identity of the individual making a request, it may request such additional information as is necessary to confirm the identity of the individual making the request. Zendesk privacy team may also request any further information, which is necessary to take action on the individual's request.

3.4 Exemptions to a Data Protection Rights Request.

3.4.1 Zendesk privacy team will not refuse to act on Data Protection Rights Request, unless it can demonstrate that an exemption applies under applicable data protection laws.

3.4.2 Zendesk privacy team may be exempt under applicable data protection laws from fulfilling the Data Protection Rights Request (or be permitted to charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested) if it can demonstrate that the individual has made a manifestly unfounded or excessive request (in particular, because of the repetitive character of the request).

3.4.5 If Zendesk decides not to take action on the Data Protection Rights Request, Zendesk will inform the individual without delay and at the latest within one (1) month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the competent data protection authority and seeking a judicial remedy.

3.5 Responding to a Data Protection Rights Request

3.5.1 Where Zendesk is the controller of the personal data that is the subject of the Data Protection Rights Request, and Zendesk has already confirmed the identity of the requestor and has sufficient information to enable it to fulfil the request (and no exemption applies under applicable data protection laws), then Zendesk will handle the Data Protection Rights Request in accordance with paragraphs 4, 5, or 6 below (as appropriate).

3.5.2 Zendesk will respond to a Data Protection Rights Request without undue delay and in no case later than one (1) month of receipt of that request. This one (1) month period may be extended by two (2) further months where necessary, taking into account the complexity and number of the requests.

4. Requests for access to personal data ("data subject access requests")

4.1 Overview

4.1.1 An individual is entitled to make a request to a controller to require it to provide the following information concerning processing of their personal data:

(a) Confirmation as to whether the controller holds and is processing personal data about them;

(b) If so, a description of the personal data and categories of personal data concerned, the envisaged period for which the personal data will be stored, the purposes for which they are being held and processed and the recipients or classes of recipients to whom the data is, or may be, disclosed by the controller;

(c) Information about the individual's right to request rectification or erasure of their personal data or to restrict or object to its processing;

(d) Information about the individual's right to lodge a complaint with a competent data protection authority;

(e) Information about the source of the personal data if it was not collected from the individual;

(f) Details about whether the personal data is subject to automated decision-making which produces legal effects concerning the individual or similarly significantly affects them; and

(g) Where personal data is transferred from Europe to a country outside of Europe, the appropriate safeguards that Zendesk has put in place relating to such transfers in accordance with applicable data protection laws.

4.1.2 An individual is also entitled to request a copy of their personal data from the controller. Where an individual makes such a request, the controller must provide that personal data to the individual in intelligible form.

4.2 Process for responding to Data Protection Access Requests.

4.2.1 If Zendesk receives a Data Protection Access Request from an individual, this will be sent to privacy@zendesk.com promptly to make an initial assessment of responsibility consistent with the requirements of paragraph 3.2 above.

4.2.2 Where Zendesk determines it is the controller of the personal data and responsible for responding to the individual directly (and that no exemption to the right of access applies under applicable data protection laws), Zendesk privacy team will arrange a search of all relevant electronic and paper filing systems.

4.2.3 The Zendesk privacy team may refer any complex cases to the Chief Privacy Officer for advice, particularly where the request includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

4.2.4 The information that must be disclosed to the individual will be collated by the Zendesk privacy team into a readily understandable format. Information required to be provided in response to a data subject access request (including the information described in paragraph 4.1.1) will be provided.

4.3 Exemptions to the right of access

4.3.1 A valid Data Protection Access Request may be refused on the following grounds:

(a) Where the Data Protection Access Request is made to a Group Member, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located.

(b) Where the personal data is held by Zendesk in non-automated form that is not or will not become part of a filing system.

(c) Where the personal data does not originate from Europe, has not been processed by any Group Member, and the provision of the personal data requires Zendesk to use disproportionate effort.

4.3.2 The Zendesk privacy team will assess each request individually to determine whether any of the above-mentioned exemptions apply.

5. Requests to correct, update or erase personal data, to restrict or cease processing personal data

5.1 If a request is received to correct, update or erase personal data, or to restrict or cease processing of an individual's personal data, this request will be sent to the Zendesk privacy team at privacy@zendesk.com promptly to make an initial assessment of responsibility consistent with the requirements in 3.2 above.

5.2 Once an initial assessment of responsibility has been made then:

5.2.1 where Zendesk is the controller of that personal data, the request will be notified to the Zendesk privacy team promptly for it to consider and handle, as appropriate in accordance with applicable data protection laws.

5.2.2 where a Customer is the controller of that personal data, Zendesk will promptly direct the data subject to the Customer/controller. Zendesk will assist the Customer to fulfil the request in accordance with the terms of its contract with the Customer.

5.3 To assist the Zendesk privacy team in assessing an individual's objection to processing of such personal data, the grounds upon which an individual may object are when:

5.3.1 Zendesk processes the personal data on grounds that:

(a) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Zendesk;

(b) the processing is necessary for the purposes of legitimate interests pursued by Zendesk or by a third party; or

(c) profiling is based on those grounds. When an individual raises an objection in such circumstances, Zendesk will no longer process the personal data unless it demonstrates compelling legitimate grounds

for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims.

5.3.2 Zendesk processes the personal data for direct marketing purposes, including profiling to the extent that it is related to direct marketing. When an individual raises an objection in such circumstances, Zendesk will no longer process the personal data for such direct marketing purposes.

5.4 To assist the Zendesk privacy team in assessing an individual's request for restriction of processing of his or her personal data, the grounds upon which an individual may request restriction are when:

5.4.1 the accuracy of the personal data is contested by the individual, for a period enabling Zendesk to verify the accuracy of the personal data;

5.4.2 the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of its use instead;

5.4.3 Zendesk no longer needs the personal data for the purposes of the processing, but it is required by the individual for the establishment, exercise or defence of legal claims; or

5.4.5 the individual has exercised his or her right to object pending the verification whether the legitimate grounds of the controller override his or her objection right.

5.5 To assist the Zendesk privacy team in assessing an individual's request for erasure of such personal data, the grounds upon which an individual may request erasure are when:

5.5.1 the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;

5.5.2 the individual withdraws consent on which the processing is based and there is no other legal ground for the processing;

5.5.3 the individual exercises its right to object to processing of such personal data and there are no overriding legitimate grounds for continue processing;

5.5.4 the personal data has been unlawfully processed;

5.5.5 the personal data has to be erased for compliance with a legal obligation to which the controller is subject; and

5.5.6 the personal data has been collected in relation to the offer of information society services to a child under the age of 16 and a parent or guardian has not consented to the processing.

5.6 When Zendesk will rectify or erase personal data, either in its capacity as controller or on instruction of a Customer when it is acting as a processor, Zendesk will notify other Group Members and any sub-processor to whom the personal data has been disclosed so that they can also update their records accordingly.

5.7 Where Zendesk acting as a controller will restrict processing of an individual's personal data, it will inform the individual before it subsequently lifts any such restriction.

5.8 If Zendesk acting as controller has made the personal data public, and is obliged to erase the personal data pursuant to a Data Protection Rights Request, it must take reasonable steps, including technical measures (taking account of available technology and the cost of implementation), to inform controllers which are processing the personal data that the individual has requested the erasure by such controllers of any links to, or copy or replication of, the personal data.

6. Right to data portability

6.1 If an individual makes a Data Protection Rights Request to Zendesk acting as controller to receive the personal data that they have provided to Zendesk in a structured, commonly used and machine-readable format and/or to transmit directly such data to another controller (where technically feasible), Zendesk's privacy team will consider and handle the request appropriately in accordance with applicable data protection laws insofar as the processing is based on that individual's consent or on the performance of, or steps taken at the request of the individual prior to entry into, a contract.

7. Questions about this Procedure

7.1 All queries relating to this Procedure are to be addressed to privacy@zendesk.com.

APPENDIX 3: PRIVACY COMPLIANCE STRUCTURE

1. Introduction

1.1. Zendesk's compliance with global data protection laws and the “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “Policies” or, respectively, the "Controller Policy" and the "Processor Policy") is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional privacy compliance structure.

2. Role of the Privacy Council

2.1. Privacy Council role: The Zendesk group of companies (“Zendesk”) have established a privacy compliance team (the “Privacy Council”) whose role is to ensure and oversee Zendesk’s compliance with data protection and information security requirements, and, along with the DPO, as further described below, are responsible for Zendesk’s compliance with the Policies. The Privacy Council, which is supported by a broader privacy team, will achieve this through the fulfilment of its responsibilities described below.

2.2. Board reporting: The Privacy Council will report and make recommendations to Zendesk senior management and the Board of Directors (the “Board”) on a regular basis, including any advice provided by the DPO, concerning:

2.2.1 Zendesk’s compliance with legal and regulatory requirements concerning data protection and information security;

2.2.2 the content, implementation and effectiveness of Zendesk’s data protection and information security policies and processes; and

2.2.3 any data protection and information security incidents experienced, the measures taken to remedy or mitigate those incidents, and the steps taken to prevent their reoccurrence.

3. Privacy Council Composition

3.1. Membership of the Privacy Council: The Privacy Council shall consist of a cross-functional group of senior staff members from various Zendesk offices. Such group is made up of the following standing corporate representatives: Chief Privacy Officer, acting through its Privacy Director, Legal Department, Marketing, Finance, Product Engineering, Product Management, Security, Human Resources (both People and Places and IT systems), and Information Technology. The Privacy Council may

invite other company departments or specific geographic head office representatives from time to time in the event that there are matters affecting the jurisdiction.

3.2. New members: Additional or replacement members of the Privacy Council shall be nominated and approved by majority approval of the Privacy Council. The Chief Privacy Officer shall have the casting vote in the event of a tied vote.

3.3. The Chief Privacy Officer: The Director of Privacy function and privacy team is authorized to carry out the responsibilities and competencies assigned to the Chief Privacy Officer under the Policies, as needed. In such instances, the Director of Privacy will seek the guidance, support, and/or approval of the Privacy Council, and the DPO, and senior leadership, as appropriate.

4. Meetings

4.1. Frequency of meetings: The Privacy Council shall meet at least once per quarter, and more often if the Privacy Council deems it necessary to carry out its responsibilities under this charter, to address a change in applicable legal or regulatory requirements or to respond to a data protection or information security incident.

4.2. Quorum and voting requirements: A majority of the members of the Privacy Council shall constitute a quorum for purposes of holding a meeting and the Privacy Council may act by a vote of a majority of the members present at such meeting. The Chief Privacy Officer shall have the casting vote in the event of a tied vote.

5. Responsibilities of the Privacy Council

5.1. Responsibilities: The Privacy Council will have the following responsibilities and authority:

5.1.1. Accountability

(a) The Privacy Council shall be accountable for managing and implementing Zendesk's compliant data protection and information security practices and procedures within Zendesk, and for ensuring that effective data protection and information security controls exist whenever Zendesk discloses personal data to a third party service provider.

(b) The Privacy Council will serve as a central contact point for any data protection related questions or concerns (via the contact e-mail address privacy@zendesk.com), whether raised by internal Zendesk staff

members or external Zendesk customers and suppliers, and will oversee the resolution of those questions or concerns.

5.1.2. Review of data protection policies and procedures

(a) The Privacy Council will evaluate, implement and oversee data protection and information security compliance practices within Zendesk that are consistent with the requirements of applicable laws and Zendesk's policies, strategies and business objectives.

(b) The Privacy Council will periodically assess Zendesk's data protection and information security compliance measures, accomplishments, and resources to ensure their continued effectiveness and identify and action improvements where necessary.

(c) The Privacy Council may discuss with senior management the data protection and information security legal and regulatory requirements applicable to Zendesk and its compliance with such requirements. After these discussions, the Privacy Council may, where it determines it appropriate, make recommendations to the Chief Privacy Counsel (who, in turn, will report any material amendments or modifications to the Board) with respect to Zendesk's data protection and information security policies and procedures to ensure ongoing compliance with applicable laws and regulations.

(d) The Privacy Council will also periodically review and assess the continued effectiveness and adequacy of this charter. Where necessary, it will recommend to the Chief Privacy Officer any amendments or modifications it believes are necessary (who, in turn, will report any material amendments or modifications to the Board).

5.1.3. Training and awareness raising

(a) The Privacy Council will be responsible for instituting and overseeing the adequacy of Zendesk's data protection training program for Zendesk staff that have access to personal data.

(a) The Privacy Council will promote privacy awareness across all business units, functional areas and geographies through data protection communications and awareness-raising initiatives.

(a) The Privacy Council shall ensure that any updates to its data protection and information security policies are communicated to staff and, where required, Zendesk customers and competent data protection authorities.

(a) To the extent necessary and appropriate, the Privacy Officer and Privacy Council are empowered to engage with the DPO with respect to training tailored to local regulatory requirements.

5.1.4. Audits

(a) The Privacy Council will provide input on audits undertaken of Zendesk's data protection and information security policies and procedures, coordinating responses to audit findings and responding to audit enquiries of its internal or external auditors, competent data protection authorities, and Zendesk customers.

5.1.5. Annual performance evaluation

(a) The Privacy Council shall once a year evaluate its own performance and report the findings and recommendations of such evaluation to the Chief Privacy Officer. The Privacy Council and Chief Privacy Officer may also engage the DPO to review such reports and engage with the highest levels of Zendesk management, including the Board of Directors.

5.1.6. Risk assessment

(a) The Privacy Council shall regularly assess whether Zendesk's data protection and information security policies, procedures and guidance expose Zendesk to any material compliance risks and, where this is the case, identify the steps that Zendesk may take to mitigate or remedy such risks.

(b) The Privacy Council may discuss with senior management legal matters (including pending or threatened litigation) that may have a material effect on Zendesk's finances, reputation or its data protection and information security compliance policies and procedures.

5.1.7. Engagement of Advisors

(a) The Privacy Council may engage independent counsel and such other advisors it deems necessary or advisable to help it perform its responsibilities for data protection and information security.

6. DPO

6.1. Role of the DPO: Zendesk has appointed the DPO, who cooperates with, advises on and supports the mission of the Privacy Council by providing information, advice, and cooperation related to processing subject to applicable data protection law. The DPO advice or questions, as applicable, is directly reported to the Board through the Privacy Council.

6.2. Responsibilities of the DPO: The DPO will have the following responsibilities and authority over processing subject to applicable data protection law:

6.2.1. Information and Advice

(a) The DPO will inform and advise Zendesk and its staff who carry out processing subject to applicable data protection law and the Policies of their respective obligations. The DPO may also be engaged by the Privacy Officer or Privacy Council to assist Zendesk in monitoring compliance at a local level, particularly, for example, to the extent that Zendesk is entering a new market or jurisdiction and tailored communication and compliance plan updates are needed to ensure compliance with the laws of the new jurisdiction whilst respecting the commitments in these Policies.

(b) The DPO will advise Zendesk and its staff who carry out DPIAs, as requested and monitor its performance.

6.2.2. Cooperation

(a) The DPO will cooperate and act as a contact point for the competent data protection authorities as required by applicable data protection law (including in case prior notification is necessary in the context of the DPIA). The Chief Privacy Officer will engage the DPO in the event that there are (i) regulatory or competent supervisory authority investigations, or (ii) local complaints from data subjects that the privacy team is unable to resolve through its standard procedures.

APPENDIX 4: PRIVACY TRAINING PROGRAM

1. Background

1.1. The “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “**Policies**” or, respectively, the "**Controller Policy**" and the "**Processor Policy**") provide a framework for the transfer of personal data between Zendesk group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how Zendesk trains its staff on the requirements of the Policies.

1.2. Zendesk trains its staff (including new hires, temporary staff and individual contractors, whose roles will bring them into contact with personal data) on the basic principles of data protection, confidentiality and information security awareness. This includes training on applicable data protection laws.

1.3. Zendesk staff who have permanent or regular access to personal data, who are involved in the collection of personal data or who are involved in the development of tools to process personal data receive additional, tailored, appropriate and up-to-date training on the Policies 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. Zendesk's privacy team has overall responsibility for privacy training at Zendesk, with input from colleagues from other functional areas including Information Security, People Ops (“HR”) and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Policies and that it is appropriate for individuals who have permanent or regular access to personal data, who are involved in the collection of personal data or in the development of tools to process personal data.

2.2. Zendesk management is committed to the delivery of privacy training courses, and will ensure that staff are required to participate, and are given appropriate time to attend such courses. Course attendance will be recorded and monitored via regular audits of the training process. These audits are performed by the Privacy Council, privacy team and/or independent third-party auditors.

2.3. In the event that these audits reveal persistent non-attendance, this will be escalated to the Chief Privacy Officer for action. Such action may include escalation of

non-attendance to the appropriate management authority within Zendesk who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participates in such training.

3. Delivery of the training courses

3.1. Zendesk has developed mandatory electronic training courses, supplemented by face to face training for employees. The courses are designed to be both informative and use-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 Zendesk staff will complete data protection training (including training on the Policies):

3.2.1. as part of their induction program;

3.2.2. as part of a regular refresher training at least once every two years (the timing of which is determined by the Zendesk Privacy Council); and

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

3.3. Certain staff will receive specialist training, including those who are involved processing activities such as employees who work in HR, Marketing, Product Development, Finance/Procurement and Customer Success 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 data protection**

4.1. Zendesk's training on the Policies will cover the following main areas:

4.1.1. Background and rationale:

a) What is data protection law?

b) What are key data protection terminology and concepts?

c) What are the data protection principles?

d) How does data protection law affect Zendesk internationally?

e) What are Zendesk's BCR Policies?

4.1.2. The Policies:

a) An explanation of the Policies

b) The scope of the Policies

c) The requirements of the Policies

d) Practical examples of how and when the Policies apply

e) The rights that the Policies give to individuals

f) The privacy implications arising from processing personal data for customers

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

a) Data Subject Access Procedure

b) Audit Protocol

c) Updating Procedure

d) Cooperation Procedure, including procedures of managing requests for access to personal data by public authorities.

e) Complaint Handling Procedure

f) Government Data Request Policy Procedure

5. Further Information

5.1.1. Any queries about training under the Policies should be addressed to privacy@zendesk.com.

APPENDIX 5: AUDIT PROTOCOL

1. Background

1.1. Zendesk'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 data transferred between the Zendesk group members ("**Group Members**").

1.2. Zendesk will audit its compliance with the Policies on a regular basis, and the purpose of this document is to describe how and when Zendesk will perform such audits.

1.3. The role of Zendesk's privacy team is to provide guidance about the collection and use of personal data subject to the Policies and to assess the collection and use of personal data by Group Members for potential privacy-related risks. The collection and use of personal data 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 Zendesk to ensure compliance with the Policies as required by the competent data protection authorities, this is only one way in which Zendesk ensures that the provisions of the Policies are observed and corrective actions taken as required.

2. Approach

2.1. Overview of audit

2.1.1. Compliance with the Policies is overseen on a day-to-day basis by the Zendesk Privacy Council. The Zendesk BCR Audit Team composed of experienced representatives of Zendesk's Legal, Information Security and Compliance teams ("**BCR Audit Team**") is responsible for performing and/or overseeing independent audits of compliance with the Policies and will ensure that such audits address all aspects of the Policies.

2.1.2. The BCR Audit Team is responsible for ensuring that any issues or instances of non-compliance are brought to the attention of the Zendesk Privacy Council and Chief Privacy Officer and that any corrective actions are determined and implemented within a reasonable time.

2.1.3. Where Zendesk acts as a processor, Customers (or auditors acting on their behalf) may audit Zendesk for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors acting on

Zendesk's behalf in respect of such processing, in accordance with the terms of the relevant Customer's contract with Zendesk.

2.2. Frequency of audit

2.2.1. Audits of compliance with the Policies are determined on the basis of the risk(s) posed by the processing activities covered by the Policies to the rights and freedoms of data subjects:

(a) at least annually in accordance with Zendesk's audit procedures; and/or

(b) specific audits (ad hoc audits) may be requested by the Chief Privacy Officer; the Board of Directors, Zendesk Privacy Council, or any other competent function in the organisation;

(c) as determined necessary by the Zendesk Privacy Council (for example, in response to a specific incident);

(d) (with respect to audits of the Processor Policy), as required by the terms of the relevant Customer's contract with Zendesk; or

(e) if there are indications of non-compliance to ensure verification of compliance with the Policies.

2.3. Scope of audit

2.3.1. The BCR 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 (including relevant plans to implement any identified corrective actions) or complaints; the period since the last review; the nature and location of the personal data processed; any corrective actions identified by the audit. The audit programme covers all aspects of the Policies (for instance, as applicable: applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the Policies, review of the contractual terms used for the transfers out of the Group to controllers or processors of data, corrective actions, etc.), including methods and action plans ensuring that corrective actions have been implemented.

2.3.2. Based on the foregoing risk analysis, the BCR Audit Team will formulate an annual audit plan in consultation with and input from the Privacy Officer and privacy team. To ensure independence of the audit from the privacy function and to ensure that the BCR Team's independent performance of their duties related to these audits, the Privacy Officer and privacy team participates in the audits to the extent that the BCR Audit Team requires documentation and completion of audit questionnaires and checklists. The BCR Audit Team is guaranteed independence as to the performance of their duties related to these audits.

2.3.3. In the event that a Customer exercises its right to audit Zendesk for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Customer's personal data. Zendesk will not provide a Customer with access to systems which process personal data of other Customers.

2.4. Auditors

2.4.1. Internal audit of the Policies (including any related procedures and controls) will be undertaken by the BCR Audit Team. In addition, Zendesk may appoint independent and experienced professional auditors acting under a duty of confidence as necessary to perform external audits of the Policies (including any related procedures and controls) relating to data privacy. Such external auditors are engaged with approval of the Privacy Officer, and Chief Legal Counsel, acting under a duty of confidence and are in possession of the required professional qualifications as necessary to perform such audits. The Privacy Officer will manage and provide quality assurance of audit work performed.

2.4.2. In the event that a Customer exercises its right to audit Zendesk for compliance with the Processor Policy, such audit may be undertaken by that Customer, or by independent and suitably experienced auditors selected by that Customer, as required by the terms of the relevant Customer's contract with Zendesk.

2.4.3. The competent data protection authorities may audit Group Members for the purpose of reviewing compliance with the Policies (including any related procedures and controls) in accordance with the terms of the Binding Corporate Rules: Cooperation Procedure.

2.5. Reporting

2.5.1. Data privacy audit reports are submitted to the Chief Privacy Officer, Zendesk International Limited's Board of Directors and, 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), to the Zendesk Group parent company Board of Directors.

2.5.2. Upon request and subject to applicable law, Zendesk will:

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

(b) subject to respect for the confidentiality and trade secrets of the information provided, to the extent that an audit relates to personal data Zendesk processes on behalf of a Customer, report the results of any audit of compliance with the Processor Policy to that Customer.

2.5.3. The Zendesk Privacy Council is responsible for liaising with the competent data protection authorities for the purpose of providing the information outlined in section 2.5.2.

APPENDIX 6: COMPLAINT HANDLING PROCEDURE

1. Background

1.1. Zendesk'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 data transferred between the Zendesk group members ("**Group Members**"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal data is processed by Zendesk under the Policies are addressed and resolved.

1.2. This procedure will be made available to individuals whose personal data is processed by Zendesk under the Controller Policy and, where Zendesk processes personal data on behalf of Customers, to those Customers (under the Processor Policy).

2. How individuals can bring complaints

2.1 Any individual may raise a data protection question, concern or complaint by contacting privacy@zendesk.com, or by post addressed to Zendesk, Inc. at 181 Fremont Street, San Francisco, California 94105, United States (to the attention of the Chief Privacy Officer).

3. Complaints where Zendesk is a controller under the Controller Policy

3.1 Who handles complaints?

3.1.1 The Zendesk privacy team will handle all questions, concerns or complaints in respect of personal data processed under the Controller Policy. The Zendesk privacy team will liaise with colleagues from relevant business and support units as appropriate to resolve such questions, concerns and complaints.

3.2 What is the response time?

3.2.1 Unless exceptional circumstances apply, Zendesk privacy team will acknowledge receipt of a question, concern or complaint to the individual concerned within five (5) business days, investigating and making a substantive response within one (1) month.

3.2.2 If, due to the complexity of the question, concern or complaint, a substantive response cannot be given within this period, the Zendesk privacy team will advise the individual accordingly and provide reasons why an extension is

necessary and a reasonable estimate (not exceeding two (2) months) for the timescale within which a response will be provided.

3.2.3 If, having reviewed the question, concern or complaint, the Zendesk privacy team does not take action that has been requested by the individual, the Zendesk privacy team will inform the individual without delay and of the reasons for not taking action and on the possibility of lodging a complaint with a competent data protection authority and seeking a judicial remedy.

3.2.4 If, having reviewed the question, concern or complaint, the Zendesk privacy team decides that it is justified, the Zendesk privacy team will provide appropriate remedy to the complainant and, as necessary, any affected internal procedures.

3.3 What happens if a complainant disputes a finding?

3.3.1 If the complainant notifies the Zendesk privacy team that it disputes any aspect of the response from the Zendesk privacy team and that it wishes to further escalate the matter within Zendesk, the Zendesk privacy team will refer the matter to the Chief Privacy Officer. The Chief Privacy Officer will review the case and advise the individual of his or her decision either to accept the original finding or to substitute a new finding. The Chief Privacy Officer will respond to the complainant within one (1) month of the receipt of the complaint. As part of the review, the Chief Privacy Officer may arrange to meet the parties to the complaint in an attempt to resolve it. At the same time, complainants can dispute the finding by lodging a complaint with a competent data protection authority and seeking judicial remedy, in parallel, if they wish to do so, in line with paragraph 5 below.

3.4 If the complaint is upheld, the Chief Privacy Officer will arrange for any necessary steps to be taken as a consequence (for example, implementing procedures to remedy the complaint and prevent recurrence).

4. Complaints where Zendesk is a processor under the Processor Policy

4.1 Communicating complaints to the customer

4.1.1 Where a complaint is brought in respect of the collection and use of personal data where Zendesk is the processor for its Customers in respect of that personal data, Zendesk will communicate the details of the complaint to the

Customer without undue delay and without handling it (unless Zendesk has agreed in the terms of its contract with the Customer to handle complaints).

4.2 What happens when a Customer ceases to exist?

4.2.2 In circumstances where a Zendesk Customer has disappeared factually, no longer exists or has become insolvent, and no successor entity has taken its place, individuals whose personal data is processed under the Processor Policy have the right to complain to Zendesk and Zendesk will handle such complaints in accordance with paragraph 3 of this Complaint Handling Procedure.

4.2.3 In such cases, individuals also have the right to complain to a competent data protection authority and/or to lodge a claim with a court of competent jurisdiction and this includes where they are not satisfied with the way in which their complaint has been resolved by Zendesk. Such complaints and proceedings will be handled in accordance with paragraph 5 of this Complaint Handling Procedure. Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

5. Right to complain to a competent data protection authority and to commence proceedings

5.1 Overview

5.1.1 Where individuals' personal data:

(a) are processed in Europe by a Group Member acting as a controller (or an internal processor for another Group Member) and/or transferred to a Group Member located outside Europe under the Controller Policy; or

(b) are processed in Europe by a Group Member acting as a processor for a Customer and/or transferred to a Group Member located outside Europe under the Processor Policy;

(c) then those individuals have certain additional rights to pursue effective remedies for their complaints, as described below.

5.1.2 The individuals described above have the right to complain to a competent data protection authority (in accordance with paragraph 5.2) and/or to commence proceedings in a court of competent jurisdiction (in accordance with paragraph 5.3), whether or not they have first complained directly to the Customer in question or to Zendesk under this Complaints Handling Procedure.

5.2 Complaint to a competent data protection authority

5.2.1 If an individual wishes to complain about Zendesk's processing of his or her personal data to a competent data protection authority, the individual may complain to the competent data protection authority in Europe:

(a) of the individual's habitual residence;

(b) of the individual's place of work; or

(c) where the alleged infringement occurred.

5.3 Proceedings before a national court

5.3.1 If an individual wishes to commence court proceedings against Zendesk, then individual may commence proceedings in Europe:

(a) in which that Group Member is established; or

(b) of individual's habitual residence.

5.3.2 Group Members accept that an individual may be represented in the proceedings by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of the GDPR, which has been properly constituted in accordance with applicable data protection law, has statutory objectives which are in the public interest, and is active in the field of the protection of individuals' rights and freedoms.

5.3.3 An individual's right to lodge proceedings before a competent court shall be without prejudice to any administrative or non-judicial remedy available to that individual, including the right to lodge a complaint with a competent data protection authority.

APPENDIX 7: COOPERATION PROCEDURE

1. Introduction

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

2. Cooperation Procedure

2.1 Where required, Zendesk will make the necessary personnel available for dialogue with a competent data protection authority in relation to the Policies.

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

2.2.1 any advice or decisions of relevant competent data protection authorities on any data protection law issues that may affect the Policies; and

2.2.3 any guidance published by competent data protection authorities in connection with Binding Corporate Rules for Processors and Binding Corporate Rules for Controllers.

2.3 Subject to applicable law, Zendesk will provide upon request information about processing covered by the Policies, and copies of the results of any audit of the Policies to a competent data protection authority.

2.4 Zendesk, including each of its Group Members, agrees that:

2.4.1 a competent data protection authority may audit, including where necessary, on-site, any Group Member over which it exercises jurisdiction for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction;

2.4.2 a competent data protection authority may audit, including where necessary, on-site, any Group Member who processes personal data for a Customer over which that competent data protection authority exercises jurisdiction for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction and with full respect to the confidentiality of the information obtained and to the trade secrets of Zendesk (unless this requirement is in conflict with local applicable law); and

2.4.3 Zendesk and each of its Group Members will cooperate with, to accept to be audited and to be inspected, including where necessary, on-site, by the competent data protection authority.

2.5 Zendesk, including its Group Members, agrees to abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Policies (unless and to the extent that Zendesk is entitled to appeal any such decision and has chosen to exercise such right of appeal).

2.6 Zendesk will agree to resolve disputes with competent data protection authority related to their supervision of Zendesk's compliance with the Policies, subject to procedural law and jurisdiction of the courts of the competent data protection authority.

APPENDIX 9: UPDATING PROCEDURE

1. Introduction

1.1 This Binding Corporate Rules: Updating Procedure sets out the way in which Zendesk will communicate changes to the "Binding Corporate Rules: Controller Policy" ("**Controller Policy**") and to the "Binding Corporate Rules: Processor Policy" ("**Processor Policy**") (together the "**Policies**") to competent data protection authorities, individual data subjects, its Customers and to the Zendesk group members ("**Group Members**") bound by the Policies.

1.2 The Zendesk Privacy Council is accountable for ensuring that the commitments made by Zendesk in this Updating Procedure are met.

2. Record keeping

2.1 Zendesk will maintain a change log setting out details of each and every revision made to the Policies.

2.2 Zendesk will also maintain an accurate and up-to-date list of Group Members that are bound by the Policies and of the sub-processors appointed by Zendesk to process personal data on behalf of Customers. This information must be made available www.zendesk.com and be provided on request to competent data protection authorities and to Customers and individuals who benefit from the Policies.

2.3 The Zendesk Privacy Council will be responsible for ensuring that the records described in this paragraph 2 are maintained and kept accurate and up-to-date.

3. Changes to the Policies

3.1 All proposed changes to the Policies must be reviewed and approved by the Chief Privacy Officer in order to ensure that a high standard of protection is maintained for the data protection rights of individuals who benefit from the Policies. No changes to the Policies shall take effect unless reviewed and approved by the Chief Privacy Officer.

3.2 The Zendesk Privacy Council will communicate, without undue delay, all changes to the Policies (including reasons that justify the changes) to the list of Group Members bound by the Policies:

3.2.1 to the Group Members bound by the Policies via written notice (which may include e-mail or posting on an internal Intranet accessible to all Group Members);

3.2.2 to Customers and the individuals who benefit from the Policies via online publication at www.zendesk.com (and, if any changes are material in nature, Zendesk will also actively communicate the material changes to Customers, in accordance with paragraph 4 below); and

3.2.3 to the competent data protection authority that was the lead authority for the purposes of granting Zendesk's BCR authorisation ("**Lead Authority**"), and any other competent data protection authorities the Lead Authority may direct, at least once a year with a brief explanation of the reasons justifying the update, including upon request of the Lead Authority, the renewal of a confirmation that Zendesk International Limited has sufficient assets, or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the Policies by Group Members. Zendesk Privacy Council will notify the Lead Authority even in instances where no changes have been made in that particular year.

4. Communication of material changes

4.1 If Zendesk makes any material changes to the Policies or to the list of Group Members bound by the Policies that affect the level of protection offered by the Policies or otherwise significantly affect the Policies (for example, by making changes to the binding nature of the Policies), it will report such changes (including the reasons that justify such changes) in advance and without undue delay to the Lead Authority.

4.2 Where a change to the Processor Policy materially affects the conditions under which Zendesk processes personal data on behalf of any Customer under the terms of its contract with Zendesk, Zendesk will also communicate such information to any affected Customer without undue delay. If such change is contrary to any term of the contract between Zendesk and that Customer:

4.2.1 Zendesk will communicate the proposed change before it is implemented, and with sufficient notice to enable affected Customers to object; and

4.2.2 Zendesk's Customer may then suspend the transfer of personal data to Zendesk and/or terminate the contract, in accordance with the terms of its contract with Zendesk.

5. New Group Members

5.1 Zendesk will ensure that all new Group Members are bound by the Policies before a transfer of personal data to them takes place.

APPENDIX 9: GOVERNMENT DATA REQUEST POLICY

1. Introduction

1.1 This Government Data Request Policy sets out Zendesk's procedure for 1) prior assessment of existing third country laws and practices, including requirements to disclose personal data or measures authorising access by public authorities; and 2) responding to a request received from a law enforcement or other government authority, including the competent supervisory authority (together the "**Requesting Authority**") to disclose personal data processed by Zendesk (hereafter "**Data Disclosure Request**") which is aligned with our Binding Corporate Rules: Government Data Request Procedure. The Policy also sets out Zendesk's notification procedure for instances where we became aware of a direct access (i.e., access to personal data without prior request, and/or approval/collaboration by Zendesk) by law enforcement or other government authority to personal data processed by Zendesk (hereafter "**Direct Access**"), which is aligned with our Binding Corporate Rules: Government Data Request Procedure.

1.2 Where Zendesk receives a Data Disclosure Request, it will handle that Data Disclosure Request in accordance with this policy. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this policy, Zendesk will comply with the relevant requirements of those applicable data protection law(s).

2. Prior assessment

2.1 Prior to Zendesk carrying out international transfers of personal data outside of Europe subject to the requirements of this Controller and/or Processor Policy, it will carry out an assessment of laws and practices of the third country of destination, including regarding Data Disclosure Request requirements or measures authorising Direct Access (including in transit), which could prevent Zendesk from fulfilling its obligations under the respective Controller/Processor Policy, such as practices that do not respect the essence of the fundamental rights and freedoms and exceed what is necessary and proportionate in a democratic society, as well as the applicable limitations and safeguards. Such assessment shall be carried out in light of the specific circumstances of the transfer, and of any envisaged onward transfer (including purposes, location and sector in which the transfer and the related processing take place, types of entities involved in the processing, categories/format of personal data transferred and transmission channels used) and determine whether additional contractual, technical or

organisational safeguards (be it during personal data transmission or at rest) are required. The assessment will be communicated by members of the privacy team to all Group Members to allow them to participate in determining additional safeguards as necessary per paragraph 2.3 below.

2.2 Zendesk will reasonably monitor future developments of laws of the country of destination to, as appropriate, to consider impacts such changes may have on the initial assessment it carried out. Group Members acting as data importers under this Controller and/or Processor Policy shall reasonably communicate such changes they become aware of to Group Members/Customers acting as data exporters and to Zendesk International Limited.

2.3 Where Zendesk determines that additional safeguards are to be put in place to address the findings of the assessment in paragraph 2.1 and/or 2.2, Group Members/Customers acting as data exporter, Zendesk International Limited, and relevant members of Privacy Council or broader privacy team, as appropriate, will identify such additional safeguards to enable relevant Group Members to fulfil their obligations under the Controller and/or Processor Policy. Group Members will implement the identified additional safeguards to the same type of transfers and these will be made available to competent data protection authority upon request.

2.4 Where the entities and functions in 2.3 determined that effective supplementary measures were needed to fulfil its obligations under the respective Controller/Processor Policy, however, it could not identify any, or if instructed by the competent supervisory authority, the Privacy Council, supported by privacy team as needed, commits to suspend the relevant transfers (including transfers for which the same assessment and reasoning would lead to the same conclusion) and inform all Group Members involved of the same to allow them to consider suspension of the same type of transfers. Following such suspension, Group Members/Customers acting as data exporters will end such personal data transfer if compliance with Controller and/or Processor Policy is not restored within one month of the suspension. Personal data, which were not subject to sufficient protections required under the Controller/Processor Policy, may be returned to the data exporter and/or destroyed, at their choice.

3. General principle on Data Disclosure Requests

3.1 As a general principle, Zendesk does not disclose personal data in response to a Data Disclosure Request unless either:

3.1.1 it is under a legal obligation to make such disclosure; or

3.1.2 taking into account the nature, context, purposes, scope and urgency of the Data Disclosure Request and the privacy rights and freedoms of any affected individuals, there is an imminent risk of serious harm that merits compliance with the Data Disclosure Requests in any event.

4. Handling of a Data Disclosure Request

4.1 A Zendesk Group Member acting as a data importer must promptly notify the data exporter, Legal Team, Privacy Officer, and Privacy Team, and, where possible, the affected individual (if necessary with the help of the data exporter) if it:

4.1.1 receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of personal data transferred pursuant to the Policies; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

4.1.2 becomes aware of any direct access by public authorities to personal data transferred pursuant to the Policies in accordance with the laws of the country of destination; such notification will include all information available to the data importer.

4.2 If Group Member acting as data importer is prohibited from notifying the data exporter and/or data subjects in line with paragraph 4.1, it will use its best efforts to obtain a waiver from such prohibition, with a view to communicate most information possible (including the fact it has been prohibited from providing such notification, if this is subject to similar restrictions) as soon as possible and will reasonably document its best efforts in order to be able to demonstrate them upon request of the data exporter.

4.3 The data importer will keep record of the available relevant information on the Data Disclosure Requests received, if any (in particular, number of requests, type of personal data requested, Requesting Authority, whether requests have been challenged and the outcome of such challenges, etc.), and regularly provide this information to the greatest degree possible, to the data exporter.

4.4 The Requesting Authority's request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Disclosure Request. Any Data Disclosure Request, however made, must be notified to the Legal Team for review.

4.5 Data Importer assisted by the Zendesk's Legal Team will carefully review each and every Data Disclosure Request and Direct Access on a case-by-case basis. The Legal Team will liaise with the Privacy Team and outside counsel as appropriate to determine the nature, context, purposes, scope and urgency of the Data Disclosure Request/Direct Access, and its validity under applicable international and country of destination laws and principles of international comity (in particular whether it remains within the powers granted to the Requesting Authority), to identify whether action may be needed to challenge the Data Disclosure Request/Direct Access, including by means of an appeal to the Requesting Authority, and/or by seeking interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits or otherwise requiring the disclosure under the applicable procedural law, as appropriate.

4.6 The data importer will document its legal assessment as well as any challenge to the Data Disclosure Request and, to the greatest extent permissible under the laws of the country of destination, make it available to the data exporter and to the Requesting Authority upon request.

4.7 The data importer will provide the minimum amount of personal data permissible, when responding to a Data Disclosure Request, based on a reasonable interpretation of the Data Disclosure Request.

5. Notice of a Data Disclosure Request/Direct Access

5.1 Notice to the customer

5.1.1 If a request concerns personal data for which a customer is the data exporter, Zendesk will ordinarily ask the Requesting Authority to make the Data Disclosure Request directly to the relevant customer. If the Requesting Authority agrees, Zendesk will support the customer in accordance with the terms of its contract to respond to the Data Disclosure Request.

5.1.2 If this is not possible (for example, because the Requesting Authority declines to make the Data Disclosure Request directly to the customer or does not know the customer's identity), Zendesk will notify and provide the customer with the

details of the Data Disclosure Request prior to disclosing any personal data, unless legally prohibited from doing so, or where an imminent risk of serious harm exists that prohibits prior notification. In such case, it will follow the procedure in paragraph 4 above.

5.1.3 If Zendesk becomes aware of a Direct Access concerning personal data for which a customer is the controller, Zendesk will notify and provide the customer with the details of such Direct Access, unless legally prohibited from doing so or where an imminent risk of serious harm exists that prohibits such notification. In such case, it will follow the procedure in paragraph 4 above.

5.2 **Providing information to the competent data protection authorities**

5.2.1 The data importer will preserve the information in paragraphs 4.2, 4.3 and 4.6 above for as long as personal data it processes is subject to BCRs and make it available to competent data protection authorities upon request.

5.2.2 Where Zendesk is prohibited from providing information the competent data protection authorities and/or suspending the request, Zendesk will use its best efforts (taking into account the nature, context, purposes, scope, and urgency of the request) to inform the Requesting Authority/authority that carried out the Direct Access about its obligations under applicable data protection law and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority/authority that carried out the Direct Access to allow notification to competent supervisory authorities, and may also, in appropriate circumstances, include seeking a court order to this effect. Zendesk will maintain, and upon reasonable request provide to competent data protection authorities, a written record of the efforts it takes, in line with its established business record maintenance practices, unless legally prohibited from doing so.

6 Transparency reports

6.1 Zendesk commits to preparing a semi-annual report (a "**Transparency Report**"), which reflects the number and type of Data Disclosure Requests it has received for the preceding six months, as may be limited by applicable law or court order. Zendesk will publish the Transparency Report on its website, and make the report available upon request to competent data protection authorities.

7 Bulk transfers

7.1 In no event will any Group Member transfer personal data to a Requesting Authority or other public authority in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.

APPENDIX 10: PERSONAL DATA BREACH NOTIFICATION PROCEDURE

1. Background

1.1 Zendesk'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 data transferred between the Zendesk group members ("**Group Members**").

1.2 The scope of this Personal Data Breach Procedure is to outline how a personal data breach affecting personal data processed subject to the Policies are notified to competent data protection authorities and affected individuals by Zendesk, where Zendesk acts as a controller, and to relevant Group Members/Customers, where Zendesk acts as a processor.

2. Processor Obligations

2.1 When affected Group Member acting as a processor becomes aware of a personal data breach, it must notify the Group Member/Customer acting as a controller for the affected personal data without undue delay.

3. Personal Data Breaches where Zendesk is a controller under the Controller Policy

3.1 A Group Member acting as a controller which suffered a personal data breach must report it to Zendesk International Ltd. and the Chief Privacy Officer without undue delay.

3.2 Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the affected individuals, the Group Member acting as a controller in cooperation with the privacy team, must without undue delay, and, where feasible, not later than 72 hours after having become aware of the personal data breach, report it to the competent data protection authority.

3.3 If personal data breach is likely to result in a high risk to the rights and freedoms of the affected individuals, the Group Member acting as a controller in cooperation with the privacy team must notify them without undue delay, unless:

3.3.1 It implemented appropriate technical and organisational measures (e.g., encryption) to affected personal data;

3.3.2 It implemented subsequent measures to ensure that such high risk to rights and freedoms of affected individuals is no longer likely to materialize; or

3.3.3 It would involve disproportionate effort. In such a case, it should issue a public communication or similar measure to effectively inform affected individuals.

4. Personal Data Breach Documentation

4.1 Privacy team will document any personal data breach. The documentation must include the facts relating to the personal data breach, its effects and the remedial action taken and shall be made available to the competent data protection authorities on request.

Appendix 11: Records of Data Processing

1. Background

1.1 Zendesk'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 data transferred between the Zendesk group members ("**Group Members**").

1.2 This Appendix outlines contents of the records, which Group Members complete with regards to processing of personal data subject to the Policies.

2. Processor Records

2.1 A Group Member acting as a processor and, where applicable, its representative

2.1.1 the name and contact details of the processor(s) and of controller(s) on behalf of which the (sub-)processor is acting;

2.1.2 where applicable, of the controller's or the processor's representative, and the DPO;

2.1.3 the categories of processing carried out on behalf of each controller;

2.1.4 where applicable, transfers of personal data to a third country, identification of that country and the documentation of suitable safeguards if transfer does not rely on appropriate safeguards or derogations available under applicable European data protection law; and

2.1.5 where possible, a general description of the technical and organisational security measures.

3. Controller Records

3.1 A Group Member acting as a controller

3.1.1 the name and contact details of the (joint/independent) controller;

3.1.2 where applicable, name and contact details of controller’s representative and the DPO;

3.1.3 the purposes of the processing;

3.1.4 a description of the categories of data subjects and of the categories of personal data;

3.1.5 the categories of recipients to whom the personal data have been or will be disclosed including in third countries;

3.1.6 where applicable, transfers of personal data to a third country, identification of that country and the documentation of suitable safeguards if transfer does not rely on appropriate safeguards or derogations available under applicable European data protection law;

3.1.7 where possible, the envisaged time limits for erasure of the different categories of data; and where possible, a general description of the technical and organisational security ; and

3.1.8 where possible, a general description of the technical and organisational security measures.

APPENDIX 12: FAIR INFORMATION DISCLOSURES

1. Background

1.1. Zendesk's Binding Corporate Rules: Controller Policy (the "**Controller Policy**") provides a framework for the transfer of personal data between Zendesk Group Members.

1.2. This Fair Information Disclosure document sets out the transparency information that Zendesk will provide to individuals when processing their personal data as a controller under the Controller Policy.

2. Information to be provided where Zendesk collects personal data directly from individuals as a controller under the Controller Policy

2.1. When Zendesk collects personal data directly from individuals, it must provide the following transparency information:

2.1.1. the identity of the data controller and its contact details;

2.1.2. the contact details of the data protection officer, where applicable;

2.1.3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

2.1.4. where the processing is based on Zendesk's or a third party's legitimate interests, the legitimate interests pursued by Zendesk or by the third party;

2.1.5. the recipients or categories of recipients of their personal data (if any); and

2.1.6. where applicable, the fact that a Group Member in Europe intends to transfer personal data to a third country or international organisation outside of Europe, and the measures that the Group Member will take to ensure the personal data remains protected in accordance with applicable law.

The table set forth below describes in further detail the information identified in this Section 2.1, among other details as to Zendesk Group Member transfers of personal data.

2.2. In addition to the information above, Zendesk will, at the time when personal data are obtained, provide individuals with the following further information necessary to ensure fair and transparent processing:

2.2.1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

2.2.2. rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling;

2.2.3. where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

2.2.4. the right to lodge a complaint with the competent supervisory authority;

2.2.5. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and of the possible consequences of failure to provide such information; and

2.2.6. the existence of automated decision-making, including profiling, and, where such decisions may have a legal effect or significantly affect the individuals whose personal data are collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for those individuals.

2.3. The transparency information described in this paragraph will be provided at the time that Zendesk obtains the personal data from the individual.

3. Information to be provided where Zendesk collects personal data about individuals from a third party source as a controller under the Controller Policy

3.1. When Zendesk collects personal data from a third party source (that is, someone other than the individual), it must provide the following transparency information:

3.1.1. the information described in paragraphs 2.1 and 2.2 above;

3.1.2. the categories of personal data that are being processed; and

3.1.3. details of the third party source from which Zendesk obtained the personal data including, if applicable, identifying whether the personal data came from publicly accessible sources.

3.2. The transparency information described in this paragraph must be provided within a reasonable period after Zendesk obtains the personal data and, at the latest, within one month, having regard to the specific circumstances in which the personal data are

processed. In addition:

3.2.1. if the personal data are to be used for communication with the individual, the transparency information described in this paragraph must be provided at the latest at the time of the first communication to that individual; and

3.2.2. if a disclosure of the personal data to another recipient is envisaged, the transparency information described in this paragraph must be provided at the latest when the personal data are first disclosed.

4. Derogations from providing transparency disclosures

4.1. The requirements to provide transparency information as described in this Fair Information Disclosures document shall not apply where and insofar as:

4.1.1. the individual already has the information;

4.1.2. the provision of such information provides impossible or would involve a disproportionate effort, and Zendesk takes appropriate measures, consistent with the requirements of applicable data protection laws, to protect the individual's rights and freedoms and legitimate interests, including by making the transparency information publicly available;

4.1.3. obtaining or disclosure is expressly laid down by applicable laws to which Zendesk is subject and these laws provide appropriate measures to protect the individual's legitimate interests;

4.1.4. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by applicable laws to which Zendesk is subject, including a statutory obligation of secrecy.

5. Material Scope of Transfers

5.1. This Section 5 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 data, the type of processing and its purposes, the categories of data subjects, and the identification of the third countries where personal data may be transferred.

5.2. Every Zendesk Group Member globally may transfer personal data to any other Zendesk Group Member globally. Consequently, every Zendesk Group Member globally may receive personal data as a result of such transfer. Zendesk Group Members transfer and process personal data under contractual requirements,

processing instructions from third parties, employment, and other business operational purposes.

5.3. Categories of data subjects. The following subsections express the categories of data subjects for purposes of disclosing the information set out in Section 5.1.

5.3.1. Website visitors, event participants, potential customers and customers.

Categories of personal data are transferred	Personal data: (i) Contact details: postal address, billing address, delivery address, phone number (fixed and mobile), email address, fax number and other personal data provided by individuals. (ii) Professional details: job title, affiliated organization, and data relating to business projects. (iii) Financial data (non-corporate customers, event attendees): bank account number, bank details, and credit card details. (iv) Order data: purchasing history, renewals, and cancellation history. (v) IT related data: IP addresses of visitors to Zendesk Group Member websites and other digital properties, online navigation data, browser type, language preferences, pixel data, cookies data, and web beacon data. (vi) Sensitive personal data: not collected unless an individual proactively provides it.
Type of processing and purpose	To: (i) market and provide Zendesk's products, services, and digital properties to individuals. (ii) process and fulfil transactions. (iii) enable individuals to access the digital properties and Zendesk services. (iv) operate, maintain, and improve Zendesk's digital properties

	and services. (v) communicate with individuals, such as by completing support requests or providing security updates. (vi) diagnose, repair, and track service and quality issues. (vii) provide outreach and training related communications including event participation.
Third countries where personal data may be transferred	The personal data described in this section may be processed in every territory where Zendesk Group Members or their processors are located. A list of Zendesk Group Member locations is available at Appendix 1 to this Controller Policy. Additional detail can be found in the Sub-processor Policy located on Zendesk's website.

5.3.2. Employee and Contractor Personal Data

Categories of personal data that are transferred	Employee personal data: (i) Contact details: postal address, billing address, delivery address, phone number (fixed and mobile), email address, fax number and other personal data provided by individuals. (ii) Professional and academic details: job title, degrees, titles, skills, language proficiency, training information, certifications, reference letter contents, employment history, and CV/résumé. (iii) Financial data: bank account details, payroll and tax related personal data, benefits and compensation personal data. (iv) National identifiers: national ID/passport number, tax ID, government identification number, driver's license, and visa or immigration status. (v) IT related data: computer ID, user ID and password, IP address, log files, software and hardware inventory, in-product and online navigation data, browser type, language preferences,

	pixel data, cookies data, and web beacon data. (vi) Lifestyle: hobbies, social activities, holiday preferences, activity preferences within internal social networks (i.e. Slack communities). (vii) Sensitive personal data: racial and ethnic data, health, criminal background check, biometric. Contractors: (i) name, contact details, education background, occupational history, government issued identification or other identification numbers and physical location. (ii) information about the contractor's employer (e.g. the agency supplying them), time worked (e.g. hours or days) for compensation purposes, (iii) contractor's preferred contact in case of emergency, or identification or travel profile data if business travel is required, and use of assets (where applicable), which may include identifying hardware data, network connection information, IP address and geographic location (such as through GPS, Bluetooth or WiFi signals). Ex-Employees: (i) details collected during employment, termination reasons, asset return, post-termination contact details (if different to during employment). Ex-Independent Contractors: (i) details collected during the term of their engagement, termination reasons, and details on asset return. Non-employee-related data: (i) beneficiary data (e.g. names, dates of birth) for life assurance benefits (where provided); name, date of birth, email address for the provision of healthcare benefits (where added to employees'

	policy); details to be found in the policy documents for the relevant service.
Type of processing and purpose	Personal data is collected, used or otherwise processed for the following illustrative purposes: (i) Human resources and personnel management. (ii) Business process execution and internal management. (iii) Health, safety, security and integrity. (iv) Organizational analysis and development, management reporting and acquisition and divestitures. (v) Compliance with law. (vi) Protecting the vital interests of staff members. Zendesk will process sensitive personal data only to the extent necessary for the following purpose(s): (i) Racial or ethnic data: For the purposes of diversity and inclusiveness monitoring and reporting conducted in accordance with applicable data protection and other laws. (ii) Data concerning health: medical and other health related benefits programs. (iii) Criminal background data: for background checking purposes in connection with the hiring of prospective staff members, conducted in accordance with applicable data protection laws. (iv) Biometric data: for security reasons, in order to enable duly authorised staff access to secure premises and systems and to enable log in capabilities, such as face ID. If Zendesk processes personal data or sensitive personal data for any other reasons not listed then it will ensure such processing is conducted in accordance with applicable data protection laws and this Controller Policy and facilitated through notices provided directly to employees.

Third countries where personal data may be transferred	The personal data described in this section may be processed in every territory where Zendesk Group Members or their processors are located. A list of Zendesk Group Member locations is available at Appendix 1 to this Controller Policy. Additional detail can be found in the Sub-processor Policy located on Zendesk's website.

5.3.3. Third Party Suppliers and Business Partners

What categories of personal data are transferred?	(i) Contact details: postal address, billing address, delivery address, phone number (fixed and mobile), email address, and fax number. (ii) Professional details: job title, affiliated organization, and data relating to business projects and contractual relationships. (iii) Financial data (i.e. sole proprietors): bank account number, bank details, and credit card details. (v) IT related data: IP addresses of visitors to Zendesk Group Member websites and other digital properties, online navigation data, browser type, language preferences, pixel data, cookies data, and web beacon data. (vi) Sensitive personal data: not collected unless an individual proactively provides it.

Type of processing and purpose	Personal data is generally collected, used or otherwise processed by Zendesk in the context of business development with third party suppliers and business partners for the following illustrative purposes: (i) Assessment, conclusion and execution of agreements with a third party supplier or business partner and the settlement of payment transactions. (ii) Business development, relationship management and marketing. (iii) Development and improvement of products and/or services. (vii) Protection of Zendesk's legal interests, claims and litigation, and compliance with law.
Third countries where personal data may be transferred	The personal data described in this section may be processed in every territory where Zendesk Group Members or their processors are located. A list of Zendesk Group Member locations is available at Appendix 1 to this Controller Policy. Additional detail can be found in the Sub-processor Policy located on Zendesk's website.

APPENDIX 13: LEGAL BASES

1. Background

1.1. Zendesk's "Binding Corporate Rules: Controller Policy" (the "Controller Policy") safeguard personal data transferred between the Zendesk group members ("Group Members"). The purpose of this Appendix is to provide list of legal bases which Group Members rely on for processing of personal data processed subject to the Controller Policy.

2. Processing of Personal Data

2.1. Group Members will ensure that individual's personal data, which are subject to applicable data protection law are processed on at least one of the following legal bases:

2.1.1. Individual's consent to the processing of their personal data for one or more specified purposes;

2.1.2. The processing is necessary for the performance of a contract to which the individual is a party or in order to take steps at the request of the individual prior to entering into a contract;

2.1.3. The processing is necessary for compliance with a legal obligation to which the controller of processed personal data is a subject;

2.1.4. The processing is necessary in order to protect the vital interests of the individual;

2.1.5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

2.1.6. The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties, except where such interests are overridden by the interests for fundamental rights and freedoms of individuals.

3. Processing of Personal Data Relating to Criminal Convictions and Offences

3.1. Group Members will process personal data relating to criminal convictions and offences or related security measures, which is processed subject to the Controller Policy, based on the legal grounds in paragraph 2 above only under the control of official authority or when authorized by applicable law providing for appropriate safeguards for the rights

and freedoms of individuals.

4. Processing of Sensitive Personal Data

4.1. Group Members will ensure that individual's sensitive personal data, which are subject to applicable data protection law are processed on at least one of the following legal bases:

4.1.1. Individual's explicit consent to the processing of their personal data for one or more specified purposes, except where applicable law provides that the processing is prohibited;

4.1.2. The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the individual in the field of employment and social security and social protection law in so far as it is authorized by applicable law or a collective agreement pursuant to applicable law providing for appropriate safeguards for the fundamental rights and the interests of the individual;

4.1.3. The processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent;

4.1.4. The processing relates to personal data which are manifestly made public by the individual;

4.1.5. The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

4.1.6. The processing is necessary for reasons of substantial public interest, on the basis of applicable law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the individual;

4.1.7. The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the staff member, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable law or pursuant to contract with a health professional and when those data are Processed by or under the responsibility of a professional

subject to the obligations of professional secrecy under applicable law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under applicable law or rules established by national competent bodies.