Binding Corporate Rules:

Controller Policy

Contents

INTRODUCTION TO THIS POLICY **4**

PART i: BACKGROUND AND ACTIONS **5**

PART II: CONTROLLER OBLIGATIONS **7**

PART III: APPENDICES **13**

INTRODUCTION TO THIS POLICY

This Binding Corporate Rules: Controller Policy ("**Policy**") establishes Zendesk's approach to compliance with European data protection law and specifically to transfers of personal information[1] between Zendesk group members ("**Group Members**") (a list of which is available at Appendix 1) when processing that information for their own purposes.

This Policy applies to all personal information processed by Zendesk as a controller whenever it is collected and used by Zendesk Group Members for their own business activities, employment administration and vendor management. As such, the personal information to which this Policy applies includes:

- CRM data about Zendesk's customers,
- human resources data about Zendesk staff members, and
- vendor data about Zendesk 's suppliers and service providers.

Group Members and their employees (including new hires and individual contractors) must comply with, and respect, this Policy when processing personal information for their own purposes.

This Policy does not apply to personal information that Zendesk processes in the course of providing services to a third party controller, which instead must be protected in accordance with the Binding Corporate Rules: Processor Policy. In particular, the content of Zendesk customers' support tickets must be processed in accordance with the Binding Corporate Rules: Processor Policy.

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

This Policy will be published on the website accessible at www.zendesk.com

[1] Personal information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in EU Directive 95/46/EC.

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

Data protection law gives people certain rights in connection with the way in which their personal information is used. If organizations do not comply with data protection law, they may be subject to sanctions and penalties imposed by the national data protection authorities and courts. When Zendesk collects and uses personal information, this activity and the personal information in question is covered and regulated by data protection law.

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

On the other hand, when an organization processes information on behalf of a third party (for example, content data processed by Zendesk on behalf of its customers), that organization is deemed to be a "*processor"* of the information. In this case, the relevant controller of the personal information (i.e., the relevant third party) will be primarily responsible for meeting the legal requirements.

This Policy describes how Zendesk will comply with data protection law in respect of processing it performs as a controller. Zendesk's Binding Corporate Rules: Processor Policy describes the standards Zendesk applies when Zendesk collects, uses or transfers personal information as a processor.

HOW DOES DATA PROTECTION LAW AFFECT COMPANY INTERNATIONALLY?

European data protection law prohibits the transfer of personal information to countries outside Europe[2] that do not ensure an adequate level of data protection. Some of the countries in which Zendesk operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

WHAT IS ZENDESK DOING ABOUT IT?

Zendesk must take proper steps to ensure that it uses personal information on an international basis in a safe and lawful manner. This Policy therefore sets out a framework to satisfy data protection law requirements and, in particular, to provide an adequate level of protection for all personal information used and collected in Europe and transferred from Group Members within Europe to Group Members outside Europe.

Zendesk will apply this Policy in all cases where it processes personal information as a controller, both manually and by automatic means. This Policy applies to all Group Members and their employees worldwide (including new hires and individual contractors), and they must comply with, and respect, this Policy when collecting and using personal information. All Group Members who collect, use or transfer personal information as a controller comply with the Rules set out in **Part II** of this Policy together with the policies and procedures set out in the appendices in **Part III** of this Policy.

Some Group Members may act as both a controller and a processor and must therefore comply with this Policy and also the Binding Corporate Rules: Processor Policy as appropriate.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Policy, your rights under this Policy, or any other data protection issues, you can contact the Chief Privacy Officer at the address below who will

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

either deal with the matter in consultation with the Zendesk Privacy Counsel or forward it to the appropriate person or department within Zendesk.

Attention:	**Chief Privacy Officer**
Email:	**privacy@zendesk.com**
Address:	**1019 Market Street, 6th Floor,** **San Francisco,** **California 94103,** **Attn: Chief Privacy Officer**

The Zendesk Privacy Council is responsible for ensuring that changes to this Policy are notified to the Group Members and to individuals whose personal information is processed by Zendesk in accordance with Appendix 8.

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

PART II: CONTROLLER OBLIGATIONS

This Policy applies in all situations where a Group Member collects, uses and transfers personal information as a controller.

Part II of this Policy is divided into three sections:

- Section A addresses the basic data protection principles that a Group Member must observe when it collects, uses and transfers personal information as a controller.
- Section B deals with the practical commitments made by Zendesk in connection with this Policy.
- Section C describes the third party beneficiary rights that Zendesk has granted to individuals under this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1 – Zendesk will always comply with local data protection law where it exists.

As an organization, Zendesk will comply with any applicable data protection legislation for the protection of personal information (e.g. in Europe, local laws implementing the EU Data Protection Directive 95/46/EC as amended or replaced from time to time). Zendesk will ensure that all personal information is collected and used in accordance with applicable local data protection law.

Where there is no law, or where the law does not meet the standards set out by the Policy, Zendesk will process personal information in accordance with the Rules in this Policy.

RULE 2 – TRANSPARENCY AND PURPOSE LIMITATION

Rule 2A – Zendesk will explain to individuals, at the time their personal information is collected, how that information will be used.

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

- the **identity** of the data controller and its contact details;
- information about an **individual's rights** to access, rectify or delete their personal information;
- the **uses** and **disclosures** made of their personal information (including the secondary uses and disclosures of the information); and
- the **recipients** or categories of recipients of their personal information.

This information will be provided when personal information 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.

Where Zendesk collects personal information for the purposes described in the introduction to this Policy, Zendesk will be the controller of that information. In all other cases, Zendesk will be a processor of

personal information disclosed to it by customers. Where Zendesk is the processor, it will comply with the requirements of the Binding Corporate Rules: Processor Policy.

Zendesk will follow this Rule 2A 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 2B – Zendesk will only obtain and use personal information for those purposes which are known to the individual or which are within their expectations and are relevant to Zendesk.

Rule 1 provides that Zendesk will comply with any applicable data protection legislation for the protection of personal information. This means that where Zendesk collects personal information in Europe and local law requires that Zendesk may only collect and use it for specific, legitimate purposes, and not use that personal information in a way that is incompatible for those purposes, Zendesk will honour these obligations.

Under Rule 2B, Zendesk will identify and make known the purposes for which personal information will be used (including the secondary uses and disclosures of the information) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

Rule 2C – Zendesk may only process personal information collected in Europe for a different or new purpose if Zendesk has a legitimate basis for doing so, consistent with the applicable law of the European country in which the personal information was collected.

If Zendesk collects personal information for a specific purpose in accordance with Rule 1 (as communicated to the individual via the relevant fair processing statement) and subsequently Zendesk wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change unless:

- it is within their expectations and they can express their concerns; or
- there is a legitimate basis for not doing so consistent with the applicable law of the European country in which the personal information was collected.

In certain cases, for example, where the processing is of sensitive personal information, or Zendesk is not satisfied that the processing is within the reasonable expectation of an individual, the individual's consent to the new uses or disclosures may be necessary.

In all cases, Zendesk must not use personal information collected in Europe in a way that is incompatible with the specific, legitimate purposes for which it was originally collected, consistent with the requirements of Rule 2B and applicable local law.

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Zendesk will keep personal information accurate and up to date.

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

Rule 3B – Zendesk will only keep personal information for as long as is necessary for the purposes for which it is collected and further processed.

Zendesk will comply with the Zendesk's record retention policies and guidelines as revised and updated from time to time.

Rule 3C – Zendesk will only keep personal information which is adequate, relevant and not excessive.

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

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Zendesk will adhere to its security policies.

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

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 implement and comply with breach notification policies as required by applicable data protection law.

Rule 4B – Zendesk will ensure that providers of services to Zendesk also adopt appropriate and equivalent security measures.

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

- to act only on Zendesk's instructions when processing that information, and
- to have in place appropriate technical and organizational security measures to safeguard the personal information.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – Zendesk will adhere to the Subject Access Request Procedure and will respond to any queries or requests made by individuals in connection with their personal information in accordance with applicable law.

Individuals may ask Zendesk to provide them with access to, and a copy of, the personal information Zendesk holds about them (including information held in both electronic and paper records). This is known as the right of subject access in European data protection law. Zendesk will follow the steps set out in the Subject Access Request Procedure (see Appendix 2) when dealing with such requests.

Rule 5B – Zendesk will deal with requests to delete, rectify or block inaccurate personal information or to cease processing personal information in accordance with the Subject Access Request Procedure.

Individuals may ask Zendesk to delete, rectify or block the personal information Zendesk holds about them, as appropriate, where it as inaccurate or incomplete. In certain circumstances, individuals may also object to the processing of their personal information. Zendesk will follow the steps set out in the Subject Access Request Procedure (see Appendix 2) in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

Rule 6 – Zendesk must not transfer personal information to third parties outside the European Economic Area without ensuring adequate protection for the information in accordance with the standards set out by this Policy.

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

RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 7 – Zendesk will only use sensitive personal information collected in Europe where the individual's express consent has been obtained, unless Zendesk has an alternative legitimate basis for doing so consistent with applicable data protection law.

Zendesk will assess whether sensitive personal information is required for the proposed use. Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and criminal convictions. In principle, Zendesk must obtain individuals' explicit consent to collect and use their sensitive personal information, unless Zendesk is otherwise required to do so by local law or has another legitimate basis for doing so consistent with the applicable law of the European country in which the personal information was collected. This permission to use sensitive personal information by Zendesk must be an explicit, freely given, specific and informed indication of the individual's wishes.

RULE8 – LEGITIMISING DIRECT MARKETING

Rule 8A – Zendesk will allow customers to opt-out of receiving marketing information.

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

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS

Rule 9 – Where decisions are made by automated means, individuals will have the right to know the logic involved in the decision and Zendesk will take necessary measures to protect the legitimate interests of individuals.

Under European data protection law, no evaluation of or decision, which produces legal effects concerning an individual, or significantly affects that individual, can be based solely on the automated processing of that individual's personal information, unless such automated processing is authorized by law or measures are taken to protect the legitimate interests of the individual.

SECTION B: PRACTICAL COMMITMENTS

RULE 10 – COMPLIANCE

Rule 10 – Zendesk will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Zendesk has appointed its Chief Privacy Officer to oversee and ensure compliance with this Policy. The Chief Privacy Officer is supported by the Zendesk Privacy Counsel, which is responsible for overseeing and enabling day-to-day compliance with this Policy at a regional and compliance level. A summary of the roles and responsibilities of Zendesk's privacy team is set out in Appendix 3.

RULE 11 – TRAINING

Rule 11 – Zendesk will provide appropriate training to employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to process personal information in accordance with the Training Requirements attached as Appendix 4.

RULE 12 – AUDIT

Rule 12 – Zendesk will comply with the Audit Protocol set out in Appendix 5.

RULE 13 – COMPLAINT HANDLING

Rule 13 – Zendesk will comply with the Complaint Handling Procedure set out in Appendix 6.

RULE 14 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 14 – Zendesk will comply with the Co-operation Procedure set out in Appendix 7.

RULE 15 – UPDATES TO THE POLICY

Rule 15 – Zendesk will comply with the Updating Procedure set out in Appendix 8.

RULE 16 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 16A – Zendesk will ensure that where the legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on its ability to comply with the Policy, Zendesk will promptly inform the Chief Privacy Officer unless otherwise prohibited by a law enforcement authority.

Rule 16B – Zendesk will ensure that where there is a conflict between the legislation applicable to it and this Policy, the Chief Privacy Officer will make a responsible decision on the action to take and will consult the data protection authority with competent jurisdiction in case of doubt.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under European data protection law, individuals benefit from certain rights to enforce this Policy where their personal information is collected and/or used by a European-based Zendesk Group Member acting as a controller (an "**EEA Entity**") and that personal information is transferred to a Zendesk Group Member located outside Europe (a "**Non-EEA Entity**").

In the event that any of the commitments under this Policy are breached, the individual's rights are as follows:

- *Complaints*: Individuals may complain to an EEA Entity in accordance with the Complaint Handling Procedure and / or to a European data protection authority in the jurisdiction of the transferring EEA Entity;

- *Proceedings*: Individuals may bring proceedings to enforce compliance with this Policy against Zendesk International Ltd before the courts of Ireland or the jurisdiction of the transferring EEA Entity;

- *Liability*: Individuals may seek appropriate redress from Zendesk International Ltd (including the remedy of any breach of this Policy by any Non-EEA Entity) and, where appropriate, receive compensation from Zendesk International Ltd for any damage suffered as a result of a breach of this Policy, in accordance with the determination of a court or other competent authority;

Individuals also have the right to obtain a copy of the Policy and the Intra-group Agreement entered into by Zendesk International Ltd or any other EEA Entity on request.

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

PART III: APPENDICES

APPENDIX 1

LIST OF GROUP MEMBERS

APPENDIX 1: LIST OF ZENDESK GROUP MEMBERS

Name of entity	Registered address	Registration number
Zendesk UK Ltd	30 Eastbourne Terrace London W2 UK	07622459
Zendesk APS	Snaregade 12, 2nd & 3rd floor DK-1205 København K Denmark	30801830
Zendesk GmbH	Rheinsberger Strasse 73, 10115 Berlin	HRB 166170 B
We Are Cloud SAS	266 place Ernest Granier, Ark Jacques Coeur 34000 Montpellier	5134683300
Zendesk, Inc.	1019 Market St San Francisco, CA 94103 United States	Delaware: 4661237
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 Pty Ltd	Level 3, 395 Collins Street, Melbourne Vic 3000 Australia	151 424 770
Kabushiki Kaisha Zendesk	15, 1 Chome, Uchikanda, 2, Chiyoda, Tokyo, Japan	0104-01-104446
Zendesk, Incorporated	30th floor, Net Park Building, 5th Ave., E-Square, Cresent Park West, The Fort, Taguig City, Metro Manila	CS201400321
Zendesk Singapore Pte. Ltd. (formerly known as Zopim Technologies Pte.)	401 Commonwealth Drive Haw Par Technocentre #07-01 Singapore 149598	201009107C
Zendesk Technologies Private Limited	Level 14 & 15, Concorde Towers, UB City, 1 Vittal Mallya Road, Bangalore – 560001.	U72200KA2016FTC093304

APPENDIX 2

SUBJECT ACCESS REQUEST PROCEDURE

Binding Corporate Rules:

Subject Access Request Procedure

Binding Corporate Rules: Subject Access Request Procedure

1. Introduction

1.1. When Zendesk collects, uses or transfers personal information for Zendesk's own purposes, Zendesk is deemed to be a *controller* of that information and is therefore primarily responsible for meeting the requirements of data protection law.

1.2. When Zendesk acts as a controller, individuals whose personal information is collected and / or used in Europe[3] (even if subsequently transferred to other Group Members) are entitled to have communicated to them whether any personal information about them is being processed by Zendesk, and if so, to obtain a copy of that personal information. This is known as the right of subject access.

1.3. In addition, all individuals whose personal information is collected and / or used in Europe by Zendesk acting as controller, and transferred between Zendesk group members ("**Group Members**") under the Binding Corporate Rules: Controller Policy, will also benefit from the right of subject access. Such subject access requests will be dealt with in accordance with the terms of this Binding Corporate Rules: Subject Access Request Procedure ("**Procedure**").

1.4. This Procedure explains how Zendesk deals with a subject access request relating to personal information which falls into the categories in sections 1.2 and 1.3 above (referred to as "**valid request**" in this Procedure).

1.5. Where a subject access request is subject to European data protection law because it is made in respect of personal information collected and/or used in Europe, such a request will be dealt with by Zendesk in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.

2. Individuals' rights

2.1. An individual making a valid subject access request to Zendesk when Zendesk is a controller of the personal information requested is entitled:

(a) to be informed whether Zendesk holds and is processing personal information about that person;

(b) to be given a description of the categories of personal information processed, the purposes for which they are being held and processed and the recipients or classes of recipients to whom the information is, or may be, disclosed by Zendesk; and

(c) to communication in intelligible form of the personal information held by Zendesk.

2.2. The request must be made in writing[4], which can include email.

2.3. Zendesk must respond to a valid request within forty (40) calendar days (or any shorter period as may be stipulated under local law) of receipt of that request.

---

[3] In this Procedure Europe means the EEA **and** Switzerland.

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

2.4. Zendesk is not obliged to comply with a subject access request unless Zendesk is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request. To assist it in fulfilling the subject access request in an efficient and timely manner, it may also communicate with the individual with a view to gathering information that will help it to locate the information which that person seeks.

3. Process

Receipt of a subject access request when Zendesk is a controller of the personal information requested.

3.1. If Zendesk receives any request from an individual for their personal information, this must be passed to the Zendesk Privacy Council at zendesk@privacy.com immediately upon receipt indicating the date on which it was received together with any other information which may assist the Zendesk Privacy Council to deal with the request.

3.2. The request does not have to be official or mention data protection law to qualify as a subject access request.

Initial steps

3.3. The Zendesk Privacy Council will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required. It will also engage Zendesk Personnel for support with handling the subject access, as required or appropriate.

3.4. The Zendesk Privacy Council will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

4. Exemptions to the right of subject access for requests made to Zendesk as a controller

4.1. A valid request may be refused on the following grounds:

(a) Where the subject access request is made to a European 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; or

(b) Where the subject access request is made to a non-European Group Member and the refusal to provide the information is consistent with the exemptions to the right of subject access under current EU data protection laws.

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

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

4.2. The Zendesk Privacy Council will assess each request individually to determine whether any of the above-mentioned exemptions applies.

5. Zendesk's search and the response

5.1. The Zendesk Privacy Council will arrange a search of all relevant electronic and paper filing systems.

5.2. The Zendesk Privacy Council 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 information may prejudice commercial confidentiality or legal proceedings.

5.3. The information requested will be collated by the Zendesk Privacy Council into a readily understandable format (internal codes or identification numbers used at Zendesk that correspond to personal information shall be translated before being disclosed). A covering letter will be prepared by the Zendesk Privacy Council which includes information required to be provided in response to a subject access request.

5.4. Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in section 2.1 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

6. Subject access requests made to Zendesk where Zendesk is a processor of the personal information requested

6.1. When Zendesk processes information on behalf of a Customer (for example, to provide a service), Zendesk is considered to be a *processor* of the information and the Customer will be primarily responsible for meeting the legal requirements as a controller. This means that when Zendesk acts as a processor, Zendesk's Customers retain the responsibility to comply with applicable data protection law.

6.2. Certain data protection obligations are passed to Zendesk in the contracts Zendesk has with its Customers and Zendesk must act in accordance with the instructions of its Customers and undertake any reasonably necessary measures to enable its Customers to comply with their duty to respect the rights of individuals. This means that if any Group Member receives a subject access request in its capacity as a processor for a Customer that Group Member must transfer such request promptly to the relevant Customer and not respond to the request unless authorized by the Customer to do so.

7. Requests for erasure, amendment or cessation of processing of personal information

7.1. If a request is received for the erasure, amendment, or cessation of processing of an individual's personal information where Zendesk is the controller for that personal information, such a request must be considered and dealt with as appropriate by the Zendesk Privacy Council.

7.2. If a request is received advising of a change in an individual's personal information where Zendesk is the controller for that personal information, such information must be rectified or updated accordingly if Zendesk is satisfied that there is a legitimate basis for doing so.

7.3. When Zendesk deletes, anonymises, updates, or corrects personal information, 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 or any sub-processor to whom the personal information has been disclosed accordingly so that they can also update their records.

7.4. If the request made to Zendesk as a controller is to cease processing that individual's personal information because the rights and freedoms of the individual are prejudiced by virtue of such

processing by Zendesk, or on the basis of other compelling legitimate grounds, the matter will be referred to the Zendesk Privacy Council to assess. Where the processing undertaken by Zendesk is required by law, the request will not be regarded as valid.

7.5. All queries relating to this Procedure are to be addressed to the Zendesk Privacy Council or at privacy@zendesk.com.

APPENDIX 3

COMPLIANCE STRUCTURE

Binding Corporate Rules:

Privacy Compliance Structure

Binding Corporate Rules: 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. Further information about Zendesk's Privacy Council is set out below and a list of the current members of the Zendesk Privacy Council is provided at Appendix 1.

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. It will achieve this through the fulfillment 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 concerning:

- Zendesk's compliance with legal and regulatory requirements concerning data protection and information security;
- the content, implementation and effectiveness of Zendesk's data protection and information security policies and processes; and
- 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 (see Appendix 1 for current members).

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.

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:

A. Accountability

- 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 information to a third party service provider.

- 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.

B. Review of data protection policies and procedures

- 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.

- 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.

- 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.

- 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).

C. Training and awareness raising

- 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 information.

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

- 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 data protection authorities.

D. Audits

- 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, data protection authorities, and Zendesk customers.

E. Annual performance evaluation

- 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.

F. Risk assessment

- 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.

- 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.

G. Engagement of Advisors

- 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.

Appendix 1: Members of the Zendesk Privacy Council

Name	Title	Department	Company Role
John Geschke	Chief Privacy Officer	Legal	Chief Legal Officer, Chief Privacy Officer, SVP Administration and Executive Sponsor of Privacy Council reporting to the Board of Directors.
Hasani Caraway	General Counsel	Legal	General Counsel responsible for legal and privacy matters.
Jason Robman	Associate General Counsel	Legal	Legal representative responsible for all commercial transactions (sales/procurement)
Rachel Tobin	Corporate Counsel, EMEA	Legal	Legal representative responsible for EMEA commercial transactions (sales/procurement)
Tom Keiser	Chief Information Officer & SVP, Technology and Operations	Technology Operations, Security and Compliance	Responsible for global technology operations including information security and compliance
Jeff Titterton	SVP, Marketing	Marketing	Responsible for Global Marketing
Steve Loyd	Director of Operations	Operations	Responsible for global operations and customer environment
Alex Brown	Vice-President	Director of IT Operations	Responsible for global information technology

Adrian McDermott	President of Products	Product	Responsible for products, product strategy and emerging businesses
Matt Price	SVP, Emerging Businesses	Product	Responsible for emerging businesses
Colum Twomey	Vice-President	Engineering	Responsible for product development and general manager of Dublin office
David Hanrahan	Vice-President	People Ops (Human Resources)	Responsible for global human resources and recruiting

APPENDIX 4

PRIVACY TRAINING REQUIREMENTS

Binding Corporate Rules:

Privacy Training Requirements

Binding Corporate Rules: Privacy Training Requirements

6. Background

6.1. 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 information 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 employees and contractors on the requirements of the Policies.

6.2. Zendesk trains employees (including new hires and contractors, whose roles will bring them into contact with personal information) on the basic principles of data protection, confidentiality and information security awareness.

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

7. Responsibility for the Privacy Training Programme

7.1. Zendesk's Privacy Council has overall responsibility for privacy training at Zendesk, with input with colleagues from other functional areas including Information Security, PeopleOps (“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 information, who are involved in the collection of personal information or in the development of tools to process personal information.

7.2. Zendesk Management supports the attendance of the privacy training courses, and are responsible for ensuring that individuals within the company are given appropriate time to attend and participate in such courses. Course attendance is monitored via regular audits of the training process. These audits are performed by the BCR Audit Team and/or independent third party auditors.

7.3. 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.

8. About the training courses

8.1. 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

8.2. All Zendesk employees will be required to complete the training:

(a) as part of their induction programme;

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

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

8.3. Certain employees will receive specialist training, including those who are involved in particular processing activities such as employees who work in HR, Marketing, Product Development, 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.

9. Training on the Policy

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

9.1.1. Background and rationale:

(a) What is data protection law?

(b) How data protection law will affect Zendesk internationally

(c) The scope of the Policies

(d) Terminology and concepts.

9.1.2. The Policies:

(a) An explanation of the Policies

(b) Practical examples

(c) The rights that the Policies give to individuals

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

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

(a) Subject Access Procedure

(b) Audit Protocol

(c) Updating Procedure

(d) Cooperation Procedure

(e) Complaint Handling Procedure

10. Further information

10.1. Any queries about training under the Policies should be addressed to Zendesk's Privacy Council at privacy@zendesk.com.

APPENDIX 5

AUDIT PROTOCOL

Binding Corporate Rules:

Audit Protocol

Binding Corporate Rules: Audit Protocol

11. Background

11.1. 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 information transferred between the Zendesk group members ("**Group Members**").

11.2. Zendesk must 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.

11.3. The role of Zendesk's Privacy Council is to provide guidance about the collection and use of personal information subject to the Policies and to assess the collection and use of personal information by Group Members for potential privacy-related risks. The collection and use of personal information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Zendesk to ensure compliance with the Policies as required by the 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.

12. Approach

Overview of audit

12.1. 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. 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.

12.2. 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.

Frequency of audit

12.3. Audits of compliance with the Policies are conducted:

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

(b) at the request of the Chief Privacy Officer; and/or

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

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

Scope of audit

12.4. 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 or complaints; the period since the last review; and the nature and location of the personal information processed.

12.5. 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. Zendesk will not provide a Customer with access to systems which process personal information of other Customers.

Auditors

12.6. 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 audits of the Policies (including any related procedures and controls) relating to data privacy.

12.7. 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.

12.8. In addition Zendesk agrees that European 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.

Reporting

12.9. Data privacy audit reports are submitted to the Chief Privacy Officer 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 parent Board of Directors.

12.10. Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Zendesk will:

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

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

12.11. The Zendesk Privacy Council is responsible for liaising with the European data protection authorities for the purpose of providing the information outlined in section 2.10.

APPENDIX 6

COMPLAINT HANDLING PROCEDURE

Binding Corporate Rules: Complaint Handing Procedure

Binding Corporate Rules: 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 information 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 information is processed by Zendesk under the Policies are dealt with.

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

2. How individuals can bring complaints

2.1. Individuals can bring complaints in writing by contacting the Zendesk Privacy Council at privacy@zendesk.com.

3. Complaints where Zendesk is a controller

Who handles complaints?

3.1. The Zendesk Privacy Council will handle all complaints arising under the Controller Policy. The Zendesk Privacy Council will liaise with colleagues from relevant business and support units as appropriate to deal the complaint.

What is the response time?

3.2. Unless exceptional circumstances apply, the Zendesk Privacy Council will acknowledge receipt of a complaint to the individual concerned within five (5) business days, investigating and making a substantive response within one month.

3.3. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Zendesk Privacy Council will advise the complainant accordingly and provide a reasonable estimate (not exceeding six (6) months) for the timescale within which a response will be provided.

What happens if a complainant disputes a finding?

3.4. If the complainant disputes the response from the Zendesk Privacy Council or any aspect of a finding and notifies the Zendesk Privacy Council, the matter will be referred to the Chief Privacy Officer. The Chief Privacy Officer will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Chief Privacy Officer will respond to the complainant within six (6) months 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.

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

3.6. 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 in accordance with the data protection laws applicable to them, whether or not they have first complained directly to Zendesk.

3.7. The jurisdiction from which the personal information was transferred will determine to which data protection authority a complaint may be made.

3.8. If the matter relates to personal information which was collected and / or used by a Group Member in Europe but then transferred to a Group Member outside Europe and an individual wants to make a claim against Zendesk, the claim may be made against the Group Member in Europe responsible for exporting the personal information.

4. Complaints where Zendesk is a processor

4.1. Where a complaint is brought in respect of the collection and use of personal information where Zendesk is the processor in respect of that information, Zendesk will communicate the details of the complaint to the Customer promptly and will act strictly in accordance with the terms of the contract between the Customer and Zendesk if the Customer requires that Zendesk investigate the complaint.

What happens when a Customer ceases to exist?

4.2. In circumstances where a Zendesk Customer has disappeared, no longer exists or has become insolvent, individuals whose personal information is collected and/or used in accordance with European data protection law and transferred between Group Members on behalf of that Customer have the right to complain to Zendesk and Zendesk will handle such complaints in accordance with section 4 of this Complaint Handling Procedure.

4.3. In such cases, individuals also have the right to complain to a European 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. Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure.

APPENDIX 7

CO-OPERATION PROCEDURE

Binding Corporate Rules: Cooperation Procedure

Binding Corporate Rules: Cooperation Procedure

1. Introduction

1.1. This Binding Corporate Rules: Cooperation Procedure sets out the way in which Zendesk will cooperate with the European[5] 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 European data protection authority in relation to the Policies.

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

(a) any advice or decisions of relevant European data protection authorities on any data protection law issues that may affect the Policies; and

(b) the views of the Article 29 Working Party in connection with Binding Corporate Rules for Processors and Binding Corporate Rules for Controllers, as outlined in its published Binding Corporate Rules guidance.

2.3. Subject to applicable law and to the respect for the confidentiality and trade secrets of the information provided, Zendesk will provide upon request copies of the results of any audit of the Policies to a relevant European data protection authority.

2.4. Zendesk agrees that:

(a) a competent European data protection authority may audit any Group Member located within its jurisdiction for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction; and

(b) a competent European data protection authority may audit any Group Member who processes personal information for a Customer established within the jurisdiction of that European data protection authority for compliance with the Policies, in accordance with the applicable data protection law(s) of that jurisdiction, 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).

2.5. Zendesk agrees to abide by a formal decision of any competent data protection authority against which a right to appeal is not exercised on any issues relating to the interpretation and application of the Policies.

[5] For the purposes of this document, references to Europe include the EEA and Switzerland.

APPENDIX 8

UPDATING PROCEDURE

CONFIDENTIAL

Binding Corporate Rules: Updating Procedure

Binding Corporate Rules: Updating Procedure

13. Introduction

13.1. 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 the European[6] data protection authorities, individual data subjects, its Customers and to the Zendesk group members ("**Group Members**") bound by the Policies.

13.2. Any reference to Zendesk in this procedure is to the Privacy Council which will ensure that the commitments made by Zendesk in this Updating Procedure are met.

14. Material changes to the Policies

14.1. Zendesk will communicate any material changes to the Policies as soon as is reasonably practical to the Data Protection Commissioner in Ireland and to any other relevant European data protection authorities.

14.2. Where a change to the Processor Policy materially affects the conditions under which Zendesk processes personal information on behalf of any Customer under the terms of its contract with Zendesk, Zendesk will also communicate such information to any affected Customer. If such change is contrary to any term of the contract between Zendesk and that Customer:

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

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

2. Administrative changes to the Policies

2.1. Zendesk will communicate changes to the Policies which:

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

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

to the Data Protection Commissioner in Ireland and to any other relevant European data protection authorities at least once a year. Zendesk will also provide a brief explanation to the Data Protection Commissioner in Ireland and to any other relevant data protection authorities of the reasons for any notified changes to the Policies.

2.2. In addition, Zendesk will make available changes to the Processor Policy which:

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

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

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

to any Customer on whose behalf Zendesk processes personal information.

3. Communicating changes to the Policies

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

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

(b) systematically to Customers and individuals who benefit from the Policies via www.zendesk.com.

3.2. Zendesk will maintain an up to date list of Group Members bound by the Policies and of the sub-processors appointed by Zendesk to process personal information on behalf of Customers. This information will be available on request from Zendesk.

4. Logging changes to the Policies

4.1. The Policies contain a change log which sets out the date each Policy is revised and the details of any revisions made. Zendesk will maintain an up-to-date list of the changes made to the Policies.

5. New Group Members

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