Version October 2020

Zendesk

Binding Corporate Rules:

Processor Policy

CONFIDENTIAL

Contents

Part 1: Introduction to this Policy **2**

Part II: Our obligations **6**

Part III: Delivering compliance in practice **13**

Part V: APPENDICES **19**

Part 1: Introduction to this Policy

This Global Binding Corporate Rules: Processor Policy (the “Policy”) establishes Zendesk's approach to compliance with 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 on behalf of a third party or another Group Member.

This Policy applies to all personal information which is collected and processed as part of the regular business activities of Zendesk in the course of providing services to a third party or another Group Member (equally referred to as the "Customer" in this Policy). This includes processing by Zendesk of personal information contained within customer support tickets uploaded onto Zendesk's platform by Zendesk's customers.

Group Members and their employees (including new hires and individual contractors) must comply with, and respect, this Policy when collecting and processing personal information in their capacity as service providers.

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 the EU General Data Protection Regulation 2016/679.

BACKGROUND AND ACTIONS

What is data protection law?

Data protection law gives individuals 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 the courts. When Zendesk collects and uses personal information to provide a service, 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 personal information on behalf of a third party (for example, content hosted on behalf of a Zendesk enterprise customer) or a different member of its corporate group (for example, to provide an intercompany service) 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 or Group Member) will be primarily responsible for meeting the legal requirements. However, there are certain direct legal obligations falling on processors too, with which Zendesk must comply.

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

How does data protection law affect Zendesk Internationally?

European data protection law does not allow the transfer of personal information to countries outside Europe[2] that do not ensure an adequate level of data protection. Some of the

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

countries in which Zendesk operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' privacy and data protection rights.

When Zendesk processes personal information as a processor, the Customer on whose behalf Zendesk processes personal information will have responsibility for complying with the European data protection laws that apply to it. As a consequence, the Customer will pass certain data protection obligations on to Zendesk in its contract appointing Zendesk as its processor. If Zendesk fails to comply with the terms of its processor appointment, this may put the Customer in breach of European data protection laws and Customer may initiate proceedings against Zendesk for breach of contract, resulting in the payment of compensation or other judicial remedies.

A Customer may enforce this Policy against any Group Member that is in breach of it. Where a non-European Group Member (or a non-European third party processor appointed by a Group Member) processes personal information for which the Customer is a controller in breach of this Processor Policy, that Customer may enforce the Processor Policy against Zendesk International Ltd. In such event, Zendesk International Ltd will be responsible for demonstrating that such Group Member (or third party processor) is not responsible for the breach, or that no such breach took place.

When a Customer transfers personal information to a Group Member for processing in accordance with this Processor Policy, a copy of this Policy shall be incorporated into the contract with that Customer. If a Customer chooses not to rely upon this Policy when transferring personal information to a Group Member outside Europe, that Customer is responsible for implementing other appropriate safeguards in accordance with European data protection laws.

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 to Group Members outside Europe, either where the personal information is collected by a Customer in Europe as a

controller, or where the personal information is collected by a Group Member in Europe as a processor.

Each of Zendesk's Customers must decide whether the commitments made by Zendesk in this Policy provide adequate safeguards for the personal information transferred to Zendesk under the terms of its contract with Zendesk. Zendesk will apply the Rules contained in this Policy whenever it acts as a processor for a Customer. Where Zendesk's Customers rely upon this Policy as providing adequate safeguards, a copy of this Policy will be incorporated into the contract with those Customers. If a Customer chooses not to rely upon this Policy that Customer is responsible for putting in place another adequate safeguard to protect the personal information.

Zendesk will apply this Policy in all cases where Zendesk processes personal information as a processor 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 as a processor. All Group Members who collect, use or transfer personal information to provide services to a third party, or who provide a service to other Group Members, in their capacity as a processor, must comply with the Rules set out in **Part II - IV** of this Policy together with the policies and procedures set out in the appendices in **Part V** 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 Global Binding Corporate Rules: Controller 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 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,** **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 V, Appendix 6.

Part II: Our obligations

This Policy applies in all situations where a Group Member collects, uses and transfers personal information as a processor. All employees and Group Members must comply with the following obligations:

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – Zendesk will ensure that processing is at all times in compliance with applicable data protection law and that compliance with this Policy will not conflict with such laws where they exist.

Zendesk will at all times comply with any applicable data protection laws (including the processor obligations under EU General Data Protection Regulation 2016/679, when applicable), as well as the standards set out in this Policy.

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

Rule 1B – Zendesk will cooperate and assist a Customer to comply with its obligations under applicable data protection laws in a reasonable time and to the extent reasonably possible.	Zendesk will, within a reasonable time and as required under the terms of the contracts with its Customers, assist Customers to comply with their obligations as controllers under applicable data protection laws. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract with a Customer, such as providing assistance to that Customer to meet its obligations to keep personal information accurate and up to date, helping the Customer to respond to data subject requests, or helping the Customer to conduct data protection impact assessments in accordance with applicable data protection laws.

RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – Zendesk will, to the extent reasonably possible, assist a Customer to comply with the requirement to explain to individuals how that information will be used.	Zendesk's Customers have a duty to explain to individuals, at the time their personal information is collected, or shortly after, how and why that information will be used in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is usually done by means of an easily accessible fair processing statement. Zendesk will provide such assistance and information to its Customers as may be required under the terms of its contracts with its Customers to comply with this requirement. For example, Zendesk may be required to provide information about any sub-processors appointed by Zendesk to process Customer personal information on its behalf under the terms of a contract with a particular Customer.
Rule 2B – Zendesk will only use personal information on behalf	Zendesk will only use personal information on behalf of its Customers and in compliance with the terms of the contracts

of, and in accordance with, the instructions of the Customer.

with its Customers.

If, for any reason, Zendesk is unable to comply with this Rule or its obligations under this Policy in respect of any contract it may have with a Customer, Zendesk will inform the Customer promptly of this fact. Zendesk's Customer may then suspend the transfer of personal information to Zendesk and/or terminate the contract, depending upon the terms of its contract with Zendesk.

In such circumstances, Zendesk will act in accordance with the instructions of that Customer and return, destroy or store the personal information, including any copies of the personal information, in a secure manner or as otherwise required, in accordance with the terms of its contract with that Customer.

In the event that legislation prevents Zendesk from returning the personal information to a Customer, or destroying it, Zendesk will inform the Customer and, in such event, maintain the confidentiality of the personal information and not process it otherwise than in accordance with the terms of its contract with that Customer.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3A – Zendesk will assist Customers to keep the personal information accurate and up to date

Zendesk will comply with any instructions from a Customer, as required under the terms of its contract with that Customer, in order to assist that Customer to comply with its obligation to keep personal information accurate and up to date.

When required to do so on instruction from a Customer, as required under the terms of its contract with that Customer,

Zendesk will update or correct personal information without undue delay.

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

In practice, when Zendesk acts for a Customer in its capacity as the provider of a helpdesk ticketing platform, Zendesk does not have access to the personal information of Customers' data subjects and so when acting in this capacity Zendesk is unlikely to be required toupdate or correct such personal information.

Rule 3B – Zendesk will assist its Customer to store personal information only for as long as is necessary for the purpose for which the information was initially collected.

Where a Customer instructs Zendesk that personal information processed on the Customer's behalf is no longer needed for the purposes for which it was collected, Zendesk will assist its Customer to erase, restrict or anonymise that personal information without delay and in accordance with the terms of its contract with the Customer.

Zendesk will notify other Group Members or any third party processors to whom the personal information has been disclosed so that they can also take such measures.

In practice, when Zendesk acts for a Customer in its capacity as the provider of a helpdesk ticketing platform, Zendesk does not have access to the personal information of Customers' data subjects and so when acting in this capacity Zendesk is unlikely to be required to erase, restrict or anonymise such personal information.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – Zendesk will assist Customers to comply with the rights of individuals.

Taking into account the nature of the processing and insofar as this is possible, Zendesk will act in accordance with the instructions of a Customer as required under the terms of its contract with that Customer to enable a Customer to comply with its duty to respect the rights of individuals.

In particular, if any Group Member receives a request from any individual wishing to exercise their data protection rights in respect of personal information for which the Customer is the controller, the Group Member will transfer such request promptly to the relevant Customer and not respond to such a request unless authorised to do so or required by law. Zendesk will follow the steps set out in the Data Subject Rights Procedure (see Appendix 2) when dealing with such requests.

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – Zendesk will put in place appropriate technical and organizational measures to safeguard personal information processed on behalf of a Customer.

European data protection law expressly requires that where Zendesk provides a service to a Customer which involves the processing of personal information, the contract between Zendesk and its Customer controls the security and organizational measures required to safeguard that information consistent with the law of the European country applicable to the Customer.

Zendesk will ensure that any employee who has access to personal information processed on behalf of a Customer is subject to a duty of confidence.

Rule 5B – Zendesk will notify a Customer of any security

Group Members will notify a Customer of any security breach in relation to personal information processed on

breach in accordance with the terms of the contract with that Customer.

behalf of that Customer without undue delay and as required to do so under the terms of the Group Member's contract with that Customer.

Rule 5C – Zendesk will only appoint, add or replace a sub-processor with authorization from the Customer and in accordance with its requirements.

Zendesk will obtain a Customer's authorization before appointing, adding or replacing a sub-processor to process personal information on its behalf. Such authorization must be obtained in accordance with the terms of the contract with the Customer.

Zendesk will ensure that up to date information regarding its appointment of sub-processors is available to those Customers in order to obtain the Customer's authorization. If, on reviewing this information, a Customer objects to the appointment of a sub-processor to process personal information on its behalf, that Customer will be entitled to take such steps as are consistent with the terms of its contract with Zendesk and as referred to in Rule 2B of this Policy.

Rule 5D – Zendesk will ensure that sub-processors undertake to comply with provisions which are consistent with (i) the terms in its contracts with a Customer and (ii) this Policy, and in particular that the sub-processor will adopt appropriate and equivalent security measures.

Group Members must only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by Zendesk in this Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their use of the personal information to which they will have access in accordance with the terms of the Group Member's contract with its Customer.

To comply with this Rule, where a sub-processor has access to personal information processed on behalf of Zendesk, Zendesk will take steps to ensure that it has in place

appropriate technical and organizational security measures to safeguard the personal information and will impose strict contractual obligations, in writing, on the sub-processor, which provide:

- commitments on the part of the sub-processor to protect the personal information to a standard consistent with those contained in this Policy (and in particular Rules 5A and 5B above) and with the terms of the contract Zendesk has with its Customer in respect of the processing in question;

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

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

Part III: Delivering compliance in practice

To ensure we follow the rules set out in our Processor Policy, in particular the obligations in Part II, Zendesk and all of its Group Members must also comply with the following practical commitments:

1. COMPLIANCE

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.

2. TRAINING

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 Privacy Training Requirements set out in Appendix 4.

3. RECORDS

Zendesk will maintain a record of the processing activities that it conducts on behalf of a Customer in accordance with European data protection laws. These records will be kept in writing (including electronic form) and Zendesk will make these records available to competent data protection authorities upon request.

4. AUDIT	Zendesk will comply with the Audit Protocol set out in Appendix 5.
5. COMPLAINTS	Zendesk will comply with the Complaint Handling Procedure set out in Appendix 6.
6. CO-OPERATION WITH DPAs	Zendesk will comply with the Co-operation Procedure set out in Appendix 7.
7. UPDATES TO THE POLICY	Zendesk will comply with the Updating Procedure set out in Appendix 8.
8. CONFLICTS BETWEEN THIS POLICY AND NATIONAL LEGISLATION	Zendesk will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Policy, Zendesk will promptly inform (unless otherwise prohibited by law): • the controller as provided for by Rule 2B (unless otherwise prohibited by a law enforcement authority); • the Chief Privacy Officer; • the appropriate data protection authority competent for the controller; and • the competent supervisory authority for the Group Member.

9. GOVERNMENT REQUESTS FOR DISCLOSURE OF PERSONAL INFORMATION

If Zendesk receives a legally binding request for disclosure of personal information which is subject to this Policy, Zendesk will:

- notify the controller promptly unless prohibited from doing so by a law enforcement authority; and
- put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the controller, unless legally prohibited from doing so or where there is an imminent risk of serious harm.

If Zendesk is legally prohibited from putting the request on hold, it will inform the requesting authority about its obligations under European data protection law and ask the authority to waive this prohibition. Where such prohibition cannot be waived, Zendesk will provide the competent data protection authorities with an annual report providing general information about any such requests for disclosure it may have received, to the extent legally permitted to do so.

PART IV: THIRD PARTY BENEFICIARY RIGHTS

Application of this Part IV

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

- those individuals' personal information are processed in the context of the activities of a third-party controller or a Group Member (acting as processor) established in Europe;
- a non-European Customer (acting as controller) or Group Member (acting as 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 (acting as processor) monitors the behaviour of those individuals, as far as their behaviour takes place in Europe;

and that Customer or Group Member (as applicable) then transfers those individuals' personal information to a non-European Group Member (or its sub-processor) for processing under this Policy.

Entitlement to effective remedies

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

- Part II (Our Obligations) of this Processor Policy;
- Paragraphs 5 (Complaints Handling), 6 (Cooperation with DPAs), 8 (Conflicts between this Policy and national legislation) and 9 (Government requests for disclosure of personal information) under Part III of this Processor Policy; and
- Part IV (Third Party Beneficiary Rights) of this Controller Policy.

Individuals' third party beneficiary rights

When this Part IV applies, the right to pursue effective remedies against Zendesk apply only if the individuals cannot bring a claim against a Customer because:

- the Customer has factually disappeared or ceased to exist in law or has become insolvent; and
- no successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law.

In such cases, individuals may exercise the following rights:

- *Complaints*: Individuals may complain to a Group Member and/or to a European data protection authority (with a choice before the data protection authority in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement), in accordance with the Complaints Handling Procedure at Appendix 6;
- *Proceedings: 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 Processor Policy have the right to receive compensation from Zendesk for the damage suffered.
- *Transparency:* Individuals also have the right to obtain a copy of the Processor Policy on request to the Chief Privacy Officer atprivacy@zendesk.com.

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 the Policy by a non-European Group Member (or any non-European sub-processor appointed by a Group Member).

In particular:

- if an individual can demonstrate damage it has suffered likely occurred because of a breach of this Policy by a non-European Group Member (or a non-European sub-processor appointed by a Group Member), Zendesk International Ltd will have the burden of proof to show that the non-European Group Member (or non-European sub-processor) is not responsible for the breach, or that no such breach took place.

- where a non-European Group Member (or any non-European third party sub-processor acting on behalf of a Group Member) fails to comply with this 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 Processor Policy;

Shared liability for breaches with controllers

Where Zendesk is engaged by a Customer to conduct processing and both are responsible for harm caused by the processing in breach of this Policy, Zendesk accepts that both Zendesk and the Customer may be held liable for the entire damage in order to ensure effective compensation of the individual.

Part V: APPENDICES

APPENDIX 1

LIST OF GROUP MEMBERS

APPENDIX 1: LIST OF ZENDESK GROUP MEMBERS

Name of entity	Registered address	Registration number
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 UK Limited	30 Eastbourne Terrace, London, W2 6LA, United Kingdom	07622459
Zendesk International Limited	55 Charlemont Place, St. Kevins, Dublin, D02 F985, Ireland	519184
Zendesk APS	Snaregade 12, 2nd & 3rd floor DK-1205 København K Denmark	30801830
Zendesk Pty., Ltd	3/395 Collins Street, Melbourne, VIC 3000 Australia	151 424 770
Kabushiki Kaisha Zendesk	2-1, Kyobashi 2-chome, Chuo-ku 20th Floor Unit: 2001-4 Tokyo, Japan, 104-0031 Japan	0104-01-104446
Zendesk Incorporated	30th floor, Net Park Building, 5th Ave., E-Square, Crescent Park West, The Fort, (Taguig City,	CS201400321

	Metro Manila, 1634 Fort Bonifacio, Philippines	
Zopim Technologies Pte.	401 Commonwealth Drive #07-01 Haw Par Technocentre, Singapore 149598	201009107C
Zendesk GmbH	Zendesk GmbH, c/o WeWork, Neue Schönhauser Straße 3 - 5	HRB 166170 B
Zendesk Singapore Pte. Ltd.	9 Straits View #10-08, Marina One West Tower	201009107C
We Are Cloud SAS	266 place Ernest Granier, Ark Jacques Coeur 34000 Montpellier	513568330 00040
Base sp. z o. o. (Base spółka z ograniczoną odpowiedzialnością)	Wyczółkowskiego 7, 30-118 Kraków, Poland	0000433377
Zendesk Technologies Private Limited	Zendesk Technologies Pvt. Limited WeWork Galaxy #43, Residency Road, Srinivas Nagar, Shanthala Nagar, Ashok Nagar, Bangalore 560 025.	U72200KA2016FTC093304
FutureSimple Inc.	Corporation Trust Center, 1209 Orange Street, Wilmington, County of New Castle, 19801	Delaware: 4659947
Zendesk Korea LLC	WeWork Gangnam Station, 373 Gangnam-daero Seocho-gu	110115-0007175
Smooch Technologies ULC	1600 - 925 West Georgia StreetVancouver, British Columbia V6C 3L2	BC1208247

CONFIDENTIAL

APPENDIX 2

DATA SUBJECT RIGHTS PROCEDURE

Binding Corporate Rules:

Data Subject Rights Procedure

Binding Corporate Rules: Data Subject Rights 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 certain data protection rights which they may exercise by making a request to Zendesk.

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 these rights. Such requests will be dealt with in accordance with the terms of this Binding Corporate Rules: Data Subject Rights Request Procedure ("**Procedure**").

1.4 This Procedure explains how Zendesk deals with a data subject rights 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 data subject rights 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 requires a higher level of protection for personal data than this Procedure, the local data protection law will prevail.

2. Individuals' rights

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

(a) **The right to access:** This is a right for an individual to obtain confirmation whether a controller processes personal information about them and, if so, to be provided with details of that personal information and access to it. The process for handling this type of request is described further in paragraphs 4-6 below;

(b) **The right to rectification:** This is a right for an individual to obtain rectification without undue delay of inaccurate personal information a controller may process about them. The process for handling this type of request is described further in paragraph 7 below;

(c) **The right to erasure:** This is a right for an individual to require a controller to erase personal information about them on certain grounds – for example, where the personal information 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 7 below.

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

(d) **The right to restriction:** This is a right for an individual to require a controller to restrict processing of personal information about them on certain grounds. The process for handling this type of request is described further in paragraph 7 below.

(e) **The right to object:** This is a right for an individual to object, on ground relating to his or her particular situation, to a controller's processing of personal information about them, if certain grounds apply. The process for handling this type of request is described further in paragraph 7 below.

(f) **The right to data portability:** This is a right for an individual to receive personal information concerning them from a controller in a structured, commonly used and machine readable format and to transmit that information to another controller, if certain grounds apply. The process for handling this type of request is described further in paragraph 8 below.

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

2.3 Zendesk must respond to a valid request without undue delay and in any case, within one (1) month (or any shorter period as may be stipulated under local law) of receipt of that request. That period may be extended by a further two (2) months where necessary, taking into account the complexity and number of requests. Zendesk will inform the individual of any such extension within one (1) month of receipt of the request, together with reasons for the delay.

2.4 Zendesk is not obliged to comply with a data subject rights 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 data subject rights 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 data subject rights request when Zendesk is a controller of the personal information requested.

3.1 If Zendesk receives any data subject rights request from an individual regarding their personal information, this must be passed to the Zendesk Privacy Council at privacy@zendesk.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 data subject rights 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 request, as required or appropriate.

---

[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.

3.4 The Zendesk Privacy Council will then contact the individual in writing to confirm receipt of the request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions applies (for example, because Zendesk can demonstrate that the individual has made a manifestly unfounded or excessive request).

Data subject requests made to Zendesk where Zendesk is a processor of the personal information

3.5 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 data subject rights requests.

3.6 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 provide assistance to enable its Customers to comply with their duty to respect the rights of individuals, insofar as this is possible and taking account of the nature of the processing undertaken by Zendesk. This means that if any Group Member receives a data subject rights 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.

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

4.1 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 information about them;

(b) If so, a description of the personal information and categories of personal information concerned, the envisaged period for which the personal information will be stored, 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 the controller;

(c) Information about the individual's right to request rectification or erasure of their personal information 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 person information if it was not collected from the individual;

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

(g) Where personal information 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 European data protection laws.

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

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

5.1 A valid subject access 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.

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

6. Zendesk's search and the response

6.1 If Zendesk receives a subject access request, the Zendesk Privacy Council will arrange a search of all relevant electronic and paper filing systems.

6.2 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.

6.3 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.

7. Requests to correct, update or erase personal information, to restrict or cease processing personal information

7.1 If a request is received to correct, update or erase personal information, or to restrict or cease 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 restrict or cease processing that individual's personal information (for example, 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.

8. Right to data portability

8.1 If an individual makes a data subject request to Zendesk acting as controller to receive the personal information that they have provided to Zendesk in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), Zendesk's Privacy Council will consider and deal with 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.

9. Questions about this Procedure

9.1 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

10. Introduction

10.1 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.

11. Role of the Privacy Council

11.1 *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.

11.2 *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.

12. Privacy Council Composition

12.1 *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).

12.2 *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.

13. Meetings

13.1 *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.

13.2 *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.

14. Responsibilities of the Privacy Council

14.1 *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.

CONFIDENTIAL

Appendix 1: Members of the Zendesk Privacy Council

Name	Title	Department	Company Role
John Geschke	Chief Legal Officer	Legal	Chief Privacy Officer and Executive Sponsor of Privacy Council reporting to the Board of Directors.
Jason Robman	Associate General Counsel	Legal	Legal representative responsible for all commercial transactions (sales/procurement)
Rachel Tobin	Associate General Counsel EMEA	Legal	Legal representative responsible for EMEA commercial transactions (sales/procurement) and privacy
Soren Abildgaard	Executive Vice President, Engineering	Engineering	Responsible for global operations and customer environment
Maarten Van Horenbeeck	Chief Information Security Officer	Security and Compliance	Responsible for global information security and compliance
Bruce Hartwell	Vice-President	Information Technology	Responsible for global information technology
Jeff Titterton	Chief Marketing Officer	Marketing	Responsible for digital marketing
Colum Twomey	Vice-President	Engineering	Responsible for product development and general manager of Dublin office
InaMarie Johnson	Chief People & Diversity Officer	People Ops (HR)	Responsible for global human resources, diversity and recruiting

Shawna Wolverton	Executive Vice President	Product Management	Responsible for Zendesk product decisions

CONFIDENTIAL

APPENDIX 4

PRIVACY TRAINING REQUIREMENTS

Binding Corporate Rules:

Privacy Training Requirements

Binding Corporate Rules: Privacy Training Requirements

15. Background

15.1 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.

15.2 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.

15.3 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.

16. Responsibility for the Privacy Training Programme

16.1 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.

16.2 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.

16.3 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.

17. About the training courses

17.1 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

17.2 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.

17.3 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.

18. Training on the Policy

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

18.1.1 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.

18.1.2 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

18.1.3 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

19. Further information

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

CONFIDENTIAL

APPENDIX 5

AUDIT PROTOCOL

Binding Corporate Rules:

Audit Protocol

Binding Corporate Rules: Audit Protocol

20. Background

20.1 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**").

20.2 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.

20.3 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.

21. Approach

Overview of audit

21.1 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.

21.2 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

21.3 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

21.4 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.

21.5 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

21.6 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.

21.7 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.

21.8 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

21.9 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.

21.10 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.

21.11 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 Handling Procedure

CONFIDENTIAL

Binding Corporate Rules: Complaint Handling Procedure

2. Background

2.1 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.

2.2 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).

3. How individuals can bring complaints

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

4. Complaints where Zendesk is a controller

Who handles complaints?

4.1 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.

5. What is the response time?

5.1 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.

5.2 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 three (3) months) for the timescale within which a response will be provided.

What happens if a complainant disputes a finding?

5.3 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 three (3) 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.

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

5.5 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.

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

5.7 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.

6. Complaints where Zendesk is a processor

6.1 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?

6.2 In circumstances where a Zendesk Customer has disappeared, no longer exists or has become insolvent, and no successor entity has taken its place, 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.

6.3 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

CONFIDENTIAL

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.

CONFIDENTIAL

APPENDIX 8

UPDATING PROCEDURE

CONFIDENTIAL

Binding Corporate Rules: Updating Procedure

Binding Corporate Rules: Updating Procedure

22. Introduction

22.1 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.

22.2 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.

23. Material changes to the Policies

23.1 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.

23.2 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.

24. Administrative changes to the Policies

24.1 Zendesk will communicate changes to the Policies which:

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

(d) 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.

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

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

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

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

to any Customer on whose behalf Zendesk processes personal information.

25. Communicating changes to the Policies

25.1 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.

25.2 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.

26. Logging changes to the Policies

26.1 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.

27. New Group Members

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