



DATA PROCESSING AGREEMENT

Visma IMS A/S

This Data Processing Agreement is entered into by _____ (“**Subscriber**”) and Zendesk, Inc. (“**Zendesk**”), each a “**Party**” and together the “**Parties**”.

1. PURPOSE

1.1 Subscriber and Zendesk have entered into a Master Subscription Agreement (“**MSA**”) pursuant to which Subscriber is granted a license to access and use the Service during the Subscription Term. In providing the Service, Zendesk will engage, on behalf of Subscriber, in the processing of Personal Data submitted to and stored within the Service by Subscriber or third parties with whom Subscriber transacts using the Service. The terms of this Data Processing Agreement (“**DPA**”) shall only apply to: (a) subject to Section 9 of this DPA, Subscribers with an active subscription to the Service(s); and (b) Personal Data within Service Data.

1.2 The Parties are entering into this DPA to ensure that the processing by Zendesk of Personal Data within the Service, by Subscriber and/or on its behalf, is done in a manner compliant with Applicable Data Protection Law.

1.3 To the extent that any terms of the MSA conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data), the terms of this DPA shall take precedence.

2. OWNERSHIP OF THE SERVICE DATA

2.1 As between the Parties, all Service Data processed under the terms of this DPA and the MSA shall remain the property of Subscriber. Under no circumstances will Zendesk act, or be deemed to act, as a “controller” (or equivalent concept) of the Service Data under any Applicable Data Protection Law.

3. OBLIGATIONS OF ZENDESK

3.1 The Parties agree that the subject matter and duration of processing performed by Zendesk under this DPA, including the nature and purpose of processing, the type of Personal Data, and categories of data subjects, shall be as described in **Annex I** of this DPA.

3.2 As part of Zendesk providing the Service to Subscriber under the MSA, Zendesk shall comply with the obligations imposed upon it under Article 28-32 of the GDPR and agrees and declares as follows:

(i) to process Personal Data in accordance with Subscriber's documented instructions as set out in the MSA and this DPA, also with regard to transfers of Personal Data to a third country or an international organisation in accordance with Article 28 (3)(a) of the GDPR, unless required to do otherwise by Union or Member State Law to which the Zendesk is subject. In any such case, Zendesk shall inform Subscriber of that legal requirement upon becoming aware of the same (except where prohibited by applicable laws);

(ii) to ensure that all staff and management of any member of the Processor Group are fully aware of their responsibilities to protect Personal Data in accordance with this DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with Article 28 (3)(b) of the GDPR;

(iii) to implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, provided that such measures shall take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved in the processing and will include those measures described in **Annex II**;

(iv) to notify Subscriber in accordance with Article 33(2) of the GDPR, without undue delay, but in any event within forty-eight (48) hours, in the event of a confirmed Personal Data Breach affecting Subscriber’s Personal Data and to take appropriate measures to mitigate its possible adverse effects;

(v) to comply with the requirements of Section 4 (*Use of Sub-processors*) when engaging a Sub-processor;



(vi) to assist Subscriber, taking into account the nature of the processing and insofar as it is commercially reasonable, to fulfil Subscriber's obligation to respond to requests from data subjects to exercise their rights under Applicable Data Protection Law (a "Data Subject Request"). In the event that Zendesk receives a Data Subject Request directly from a data subject, it shall, unless prohibited by law, direct the data subject to the Subscriber. In the event Subscriber is unable to address the Data Subject Request, taking into account the nature of the processing and the information available to Zendesk, Zendesk shall, on Subscriber's request and at Subscriber's reasonable expense (scoped prior to Zendesk's response to the Data Subject Request), address the Data Subject Request, as required under the Applicable Data Protection Law;

(vii) upon request, to provide Subscriber with commercially reasonable information and assistance, taking into account the nature of the processing and the information available to Zendesk, to help Subscriber to conduct any data protection impact assessment, data transfer impact assessment or Supervisor consultation it is required to conduct under Applicable Data Protection Law;

(viii) upon termination of Subscriber's access to and use of the Service, to comply with the requirements of Section 8 of this DPA (*Return and Destruction of Personal Data*);

(ix) to comply with the requirements of Section 5 of this DPA (*Audit*) in order to make available to Subscriber information that demonstrates Zendesk's compliance with this DPA; and

(x) to appoint a security officer who will act as a point of contact for Subscriber, and coordinate and control security compliance with this DPA, including the measures detailed in **Annex II**.

3.3 Zendesk shall immediately inform Subscriber if, in its opinion, Subscriber's processing instructions infringe any law or regulation. In such event, Zendesk is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation.

4. USE OF SUB-PROCESSORS

4.1 Subscriber hereby confirms its general written authorisation for Zendesk's use of the Sub-processors listed at <https://help.zendesk.com/hc/en-us/articles/229138187-Subprocessors-and-Subcontractors> ("**Sub-processor Policy**") in accordance with Article 28 of the GDPR to assist Zendesk in providing the Service and processing Personal Data, provided that such Sub-processors:

(i) agree to act only on Zendesk's instructions when processing the Personal Data, which instructions shall be consistent with Subscriber's processing instructions to Zendesk;

(ii) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including implementing and maintaining appropriate technical and organisational measures to protect the Personal Data they process consistent with the Security Standards described in **Annex III** to this DPA, as applicable.

4.2 Zendesk shall remain liable to Subscriber for the subcontracted processing services of any of its Sub-processors under this DPA. Zendesk shall update the Sub-processor Policy on its Website of any Sub-processor to be appointed at least thirty (30) days prior to such change. Subscriber may sign up to receive email notification of any such changes on our Website.

4.3 In the event that Subscriber objects to the processing of its Personal Data by any newly appointed Sub-processor as described in Section 4.2, it shall inform Zendesk within thirty (30) days following the update of its Website Sub-processor Policy above. In such event, Zendesk will either (a) instruct the Sub-processor to cease the processing of Subscriber's Personal Data, in which event this DPA shall continue unaffected, or (b) allow Subscriber to terminate this DPA and any related services agreement with Zendesk immediately and provide it with a pro rata reimbursement of any sums paid in advance for Services to be provided, but not yet received by Subscriber as of the effective date of termination.

4.4 The Service provides links to integrations with Non-Zendesk Services, including, without limitation, certain Non-Zendesk Services which may be integrated directly into Subscriber's account or instance in the Service. If Subscriber elects to enable, access, or use such Non-Zendesk Services, its access and use of such Non-Zendesk Services is governed solely by the terms and conditions and privacy policies of such Non-Zendesk Services, and Zendesk does not endorse and is not responsible or liable for, and makes no representations as to any aspect of such Non-Zendesk Services, including, without limitation, their content or the manner in which



they handle Service Data (including Personal Data) or any interaction between Subscriber and the provider of such Non-Zendesk Services. The providers of Non-Zendesk Services shall not be deemed Sub-processors for any purpose under this DPA.

5. AUDIT

5.1 The Parties acknowledge that, excluding Innovation Services, Zendesk uses external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which Zendesk provides its data processing services. This audit:

- (i) will be performed at least annually;
- (ii) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;
- (iii) will be performed by independent third-party security professionals at Zendesk's selection and expense; and
- (iv) will result in the generation of an audit report affirming that Zendesk's data security controls achieve prevailing industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) or such other alternative standards that are substantially equivalent to ISO 27001 ("**Report**").

5.2 At Subscriber's written request and without charge, Zendesk will provide Subscriber with a confidential summary of the Report ("**Summary Report**") so Subscriber can reasonably verify Zendesk's compliance with the security and audit obligations under this DPA. The Summary Report will constitute Zendesk's Confidential Information under the confidentiality provisions of Zendesk's MSA.

5.3 This Section 5.3 applies only to the extent Zendesk is unable to demonstrate compliance with the EU SCCs (as defined hereinafter) through appropriate documentation and information on the processing activities carried out on behalf of Subscriber, taking into account Zendesk's certifications. By providing a notice to security@zendesk.com and privacy@zendesk.com, Subscriber may ask to exercise the right to perform an audit during normal business hours at Zendesk's premises or physical facilities for the purposes of demonstrating compliance with the EU SCCs (as defined hereinafter) and processing activities and shall be limited to data relevant to Subscriber. Zendesk will make commercially reasonable efforts to comply with such request. The Parties will mutually agree in advance and in good faith the terms of such audit, provided that:

- (i) if the request could, in Zendesk's reasonable opinion, create a risk for another Zendesk customer's environment, Zendesk and the Subscriber will agree on an alternative way to address the request to provide the Subscriber a similar level of assurance. For the avoidance of doubt, the Subscriber acknowledges that the granting of potential access as stated in this DPA shall in no way be deemed to constitute access, or potential access to the Service Data of other subscribers, either in aggregated storage at rest, or in multi-tenant data streams during processing; and
- (ii) unless otherwise agreed in writing by the Parties, Subscriber shall reimburse Zendesk for any time expended for any such on-site access at Zendesk's then-current professional services rates, which shall be made available to Subscriber upon request.

6. INTERNATIONAL DATA EXPORTS

6.1 Subscriber acknowledges that Zendesk and its Sub-processors may process Personal Data in countries that are outside of the EEA, United Kingdom, and Switzerland ("**European Countries**"). This will apply even where Subscriber has agreed with Zendesk to host Personal Data in the EEA in accordance with Zendesk's Regional Data Hosting Policy if such non-European Countries processing is necessary to provide support-related or other services requested by Subscriber. If Personal Data is transferred to a country or territory outside of European Countries, then such transfer will only take place if: (a) the country ensures an adequate level of data protection; (b) one of the conditions listed in Article 46 GDPR (or its equivalent under any successor legislation) is satisfied; or (c) the Personal Data is transferred on the basis of the Zendesk Binding Corporate Rules as set out in Section 6.2 and which establish appropriate safeguards for such Personal Data and are legally binding on the Zendesk Group.

6.2 Binding Corporate Rules

Where Zendesk processes or permits any Sub-processor within the Processor Group to process Personal Data outside the EEA or



Switzerland, Zendesk shall comply in full with the requirements of Zendesk's Binding Corporate Rules in order to provide adequate protections for the Personal Data that it processes on behalf of Subscriber, which are available at <https://d1eipm3vz40hy0.cloudfront.net/pdf/ZENDESK-BCR-Controller-Policy.pdf> and <https://d1eipm3vz40hy0.cloudfront.net/pdf/ZENDESK%20-%20BCR%20Processor%20Policy.pdf>. In the event the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in the following order: (1) Zendesk's Binding Corporate Rules; (2) the applicable Standard Contractual Clauses; and if neither (1) or (2) is applicable, then other applicable data transfer mechanisms permitted under Applicable Data Protection Law.

6.3 Standard Contractual Clauses

Where Zendesk processes Personal Data in non-EEA countries, Zendesk shall comply with the EU Commission's Standard Contractual Clauses (annexed to EU Commission Decision 2021/914/EU of 4 June 2021) (the "EU SCCs") which, if Clause 6.2 (*Binding Corporate Rules*) does not apply, shall be entered into and incorporated into this DPA by this reference and completed as follows:

(i) Module 2 (Controller to Processor) will apply where Subscriber is a controller of Service Data and Zendesk is a processor of Service Data; Module 3 (Processor to Processor) will apply where Subscriber is a processor of Service Data and Zendesk is a processor of Service Data. For each Module, where applicable:

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 4 of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 12, any claims brought under the EU SCCs shall be subject to the terms and conditions set forth in the MSA. In no event shall any party limit its liability with respect to any data subject rights under the EU SCCs.

(vi) in Clause 17, Option 1 will apply, will be governed by Irish law;

(vii) in Clause 18(b), disputes shall be resolved before the courts of Dublin;

(viii) **Annex I** of the EU SCCs shall be deemed completed with the information set out in **Annex I** to this DPA; and

(ix) **Annex II** of the EU SCCs shall be deemed completed with the information set out in **Annex II** to this DPA.

Nothing in the interpretations in this Section 6.3 is intended to conflict with either Party's rights or responsibilities under the EU SCCs and, in the event of any such conflict, the EU SCCs shall prevail.

6.4 To the extent any export from or processing of Personal Data outside the United Kingdom is subject to Applicable Data Protection Law in the United Kingdom (including UK GDPR and Data Protection Act 2018) ("**UK Data Protection Laws**"), for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU ("**Prior SCCs**"), the Prior SCCs shall apply between Subscriber and Zendesk on the following basis: (i) Appendix I and II shall be deemed completed with the relevant information set out in **Annex I and II** to this DPA; (ii) references in the Prior SCCs to "the law of the Member State in which the data exporter is established" shall be deemed to mean "the laws of England and Wales"; (iii) the optional illustrative indemnification clause will not apply; and (iv) any other obligation in the Prior SCCs determined by the Member State in which the data exporter is established shall be deemed to refer to an obligation under UK Data Protection Laws. Where the Prior SCCs do not apply and the Parties are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the UK subject to completion of a UK Addendum to the EU SCCs issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"), then the EU SCCs, completed as set out above in Section 6.3(i)-(ix) of this DPA shall also apply to transfers of such Personal Data, subject to the provision that the UK Addendum shall be deemed executed between Zendesk and Subscriber, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data. If neither the Prior SCCs or UK Addendum with EU SCCs applies,



then the Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK Data Protection Laws without undue delay.

6.5 Zendesk continues to participate in and comply with the commitments to which it has certified under the EU-U.S. and Swiss-U.S Privacy Shield Frameworks; however, Zendesk does not currently rely on these frameworks as a basis for transfer of Personal Data.

7. OBLIGATIONS OF SUBSCRIBER

7.1 As part of Subscriber receiving the Service under the MSA, Subscriber agrees to abide by its obligations under Applicable Data Protection Law.

8. RETURN AND DESTRUCTION OF PERSONAL DATA

8.1 Upon termination of Subscriber's access to and use of the Service, Zendesk will within thirty (30) days following such termination, at the choice of the Subscriber either: (a) permit Subscriber to export its Service Data, at its expense; or (b) delete all Service Data in accordance with the capabilities of the Service and Article 28 (3)(g) of the GDPR. Following such period, Zendesk shall delete all Service Data stored or processed by Zendesk on behalf of Subscriber in accordance with Zendesk's deletion policies and procedures. Subscriber expressly consents to such deletion.

9. DURATION

9.1 This DPA will remain in force as long as Zendesk processes Personal Data on behalf of Subscriber under the MSA.

10. LIMITATION OF LIABILITY

10.1 This DPA shall be subject to the limitations of liability agreed between the Parties set forth in the MSA and any reference to the liability of a Party means that Party and its Affiliates in the aggregate. For the avoidance of doubt, Subscriber acknowledges and agrees that Zendesk's total liability for all claims from Subscriber or its Affiliates arising out of or related to the MSA and this Agreement shall apply in aggregate for all claims under both the MSA and this DPA. For the avoidance of doubt, this section shall not be construed as limiting the liability of either Party with respect to claims brought by data subjects.

11. MISCELLANEOUS

11.1 This DPA may not be amended or modified except in writing and signed by both Parties. This DPA may be executed in counterparts. Each Party's rights and obligations concerning assignment and delegation under this DPA shall be as described in the MSA. Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns. This DPA, along with the MSA constitute the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject-matter.

12. GOVERNING LAW AND JURISDICTION

12.1 This DPA is governed by the laws of Ireland, and is subject to the exclusive jurisdiction of the courts of Dublin. Notices under this DPA shall be sent in accordance with the notice provisions of the MSA.

13. DEFINITIONS

Unless otherwise defined in the MSA or the Reseller Subscription Services Agreement, as applicable, all terms used in this DPA shall have the meanings given to them below. "**Personal Data**", "**Personal Data Breach**", "**processing**", "**process**", "**processor**", "**controller**", and "**data subject**" shall have the same meaning as in the Applicable Data Protection Law and may be lowercase or capitalised herein.



13.1 Applicable Data Protection Law: means, in addition to the regulations applicable to certain jurisdictions referred to in the Region-Specific Terms set out in the MSA, the following data protection law(s), as applicable, including any subsequent amendments, modifications and revisions thereto: (i) the EU Regulation 2016/679 entitled “On the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“GDPR”) and any applicable national laws implemented by European Economic Area (“EEA”) member countries; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded); and (iii) the Data Protection Act 2018 (c. 12) of the United Kingdom.

13.2 Subscriber: means the first party named above. However, in the event Zendesk is required to process Personal Data on the request of an Affiliate of Subscriber, such Affiliate shall also be deemed as the “Subscriber”. Any reference to the Subscriber within this DPA, unless otherwise specified, shall include Subscriber and its Affiliates.

13.3 Reseller Subscription Services Agreement: means the subscription services agreement applicable to customers of Zendesk resellers. However, for the purpose of this DPA, any reference to the Master Subscription Services Agreement should be considered a reference to the Reseller Subscription Services Agreement for customers of Zendesk resellers.

13.4 Processor Group: means Zendesk and any entity which controls, is controlled by, or is under common control with, Zendesk.

13.5 Service Data: means a subset of Confidential Information comprised of electronic data, text, messages, communications or other materials submitted to and stored within the Service by Subscriber, its Agents and End-Users in connection with Subscriber’s use of such Service, including, without limitation, Personal Data.

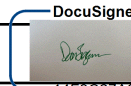

13.6 Sub-processor: means any third party data processor engaged by Zendesk, including entities from the Processor Group, who receives Personal Data from Zendesk for processing on behalf of Subscriber and in accordance with Subscriber’s instructions (as communicated by Zendesk) and the terms of its written subcontract.

13.7 Supervisor: means any data protection supervisory authority as defined in the GDPR with competence over Subscriber and Zendesk’s processing of Personal Data.

13.8 Website: means the webpage available at: <https://www.zendesk.com/company/agreements-and-terms/>.

13.9 Zendesk’s Regional Data Hosting Policy: means the policy located at: <https://support.zendesk.com/hc/en-us/articles/360022185194-Regional-Data-Hosting-Policy>

IN WITNESS WHEREOF, the Parties hereto have executed this DPA by their duly authorised officers or representatives as of the last date of execution below (“Effective Date”).

Subscriber: Visma IMS A/S		Zendesk, Inc.:	
BY:		BY:	
NAME:	Dan Thordahl Jørgensen	NAME:	Shanti Ariker
TITLE:	Managing Director	TITLE:	SVP, General Counsel
DATE:	11/18/2021	DATE:	11/18/2021
EMAIL:	dtj@ims.dk	EMAIL:	Attn: Zendesk Privacy Team and DPO privacy@zendesk.com





ANNEX I
Details of Processing

Data Exporter: Subscriber

Contact Details: Provided in the DPA signature block.

Data Exporter Role: Subscriber is Processor.

Data Importer: Zendesk, Inc.

Contact Details: Provided in the DPA signature block.

Data Importer Role: Zendesk is a processor.

1. Nature and Purpose of the Processing: Zendesk will process Personal Data in the course of providing Service(s) under the MSA, which may include operation of a cloud-based customer services platform. Additional information about Zendesk Services is available at www.zendesk.com. Zendesk will process Personal Data as a processor in accordance with Subscriber's instructions.

2. Processing Activities: Personal Data contained in Service Data will be subject to the hosting and processing activities of providing the Services.

3. Duration of Processing: The processing of Personal Data shall endure for the duration of the Subscription Term in the MSA and this DPA on a continuous basis.

4. Data Subjects: Subscriber may, at its sole discretion, submit Personal Data to the Service(s), which may include, but is not limited to, the following categories of data subjects: employees (including contractors and temporary employees), relatives of employees, customers, prospective customers, service providers, business partners, vendors, End-Users, advisors (all of whom are natural persons) of Subscriber and any natural person(s) authorized by Subscriber to use the Service(s).

5. Categories of Personal Data: Subscriber may, at its sole discretion, transfer Personal Data to the Zendesk Service(s) which may include, but is not limited to, the following categories of Personal Data: first and last name, email address, title, position, employer, contact information (company, email, phone numbers, physical address), date of birth, gender, communications (telephone recordings, voicemail), and customer service information.

6. Special Categories of Data (if applicable): Sensitive Data may, from time to time, be included in processing via the Service(s) where Subscriber or its End-Users choose to include Sensitive Data within the Service(s). Subscriber is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Subscriber's End-Users to transmit or process any Sensitive Data via the Service(s).

7. Retention: Zendesk will process and retain Personal Data in accordance with the Section 8 (*Return and Destruction of Personal Data*) of this DPA and Zendesk Data Deletion Policy incorporated by reference here: <https://support.zendesk.com/hc/en-us/articles/360022185214-Zendesk-Service-Data-Deletion-Policy>



ANNEX II

Zendesk Technical and Organisational Security Measures - Enterprise Services

The full text of Zendesk's technical and organisational measures to protect Service Data for Enterprise Services is available at <https://www.zendesk.com/product/zendesk-security/> and <https://www.zendesk.com/company/agreements-and-terms/protect-service-data-enterprise-services/>. Zendesk reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this document.

1. Information Security Program and Team: The Zendesk security program includes documented policies and standards of administrative, technical, physical and organisational safeguards, which govern the handling of Service Data in compliance with applicable law. The security program is designed to protect the confidentiality and integrity of Service Data, appropriate to the nature, scope, context and purposes of processing and the risks involved in the processing for the data subjects. Zendesk maintains a globally distributed security team on call 24/7 to respond to security alerts and events.

2. Security Certifications: Zendesk holds the following security-related certifications from independent third-party auditors: **SOC 2 Type II, ISO 27001:2013, and ISO 27018:2014.**

3. Physical Access Controls: Zendesk takes reasonable measures, such as security personnel and secured buildings, to prevent unauthorised persons from gaining physical access to Service Data and validate third parties operating data centers on our behalf are adhering to such controls.

4. System Access Controls: Zendesk takes reasonable measures to prevent Service Data from being used without authorization. These controls vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

5. Data Access Controls: Zendesk takes reasonable measures to ensure Service Data is accessible and manageable only by properly authorised staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Service Data to which they have privilege of access; and, that Service Data cannot be read, copied, modified or removed without authorisation in the course of processing.

6. Transmission Controls: Zendesk takes reasonable measures to ensure the ability to check and establish which entities the transfer of Service Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport. Service Data is encrypted in transit over public networks when communicating with Zendesk user interfaces (UIs) and application programming interface (APIs) via industry standard HTTPS/TLS (TLS 1.2 or higher). Exceptions to encryption in transit may include any non-Zendesk Service that does not support encryption, which data controller may link to through the Enterprise Services at its election. Service Data is encrypted at rest by Zendesk's Sub-processor and managed services provider, Amazon Web Services Inc., via AES-256.

7. Input Controls: Zendesk takes reasonable measures to provide the ability to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed; and, any transfer of Service Data to a third-party service provider is made via a secure transmission.



8. Logical Separation: Data from different Zendesk’s subscriber environments is logically segregated on systems managed by Zendesk to ensure that Service Data that is collected by different data controllers is segregated from one another.

9. No Backdoors: Zendesk has not built any backdoors or other methods into its Services to allow government authorities to circumvent its security measures to gain access to Service Data.

10. Data Center Architecture and Security: Zendesk hosts Service Data primarily in AWS data centers that have been certified as ISO 27001, PCI DSS Service Provider Level 1, and/or SOC2 compliant. AWS infrastructure services include backup power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data. AWS on-site security includes a number of features, such as, security guards, fencing, securing feeds, intrusion detection technology, and other security measures. More details on AWS controls can be found at: <https://aws.amazon.com/security>

11. Network Architecture and Security: Zendesk systems are housed in zones to commensurate with their security, depending on function, information classification, and risk. Our network security architecture consists of multiple zones with more sensitive systems, like database servers, in our most trusted zones. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilised between the internet and internally between the different zones of trust. Our network is protected through the use of key AWS security services, regular audits, and network intelligence technologies, which monitor and/or block known malicious traffic and network attacks. Zendesk utilises network security scanning to provide quick identification of potentially vulnerable systems, in addition to our extensive internal scanning and testing program. Zendesk also participates in several threat intelligence sharing programs to monitor threats posted to these threat intelligence networks and take action based on risk. Zendesk has a multi-layer approach to DDoS mitigation, utilising network edge defenses, along with scaling and protection tools.

12. Testing, Monitoring, and Logging: Each year, Zendesk employs third-party security experts to perform a broad penetration test across the Zendesk Protection and Corporate Networks. Zendesk utilises a Security Incident Event Management (SIEM) system, which gathers logs from important network devices and host systems. The SIEM alerts on triggers that notify the Security team based on correlated events for investigation and response. Service ingress and egress points are instrumented and monitored to detect anomalous behavior, including 24/7 system monitoring.

13. Data Hosting Location: Zendesk offers Subscribers an option to elect where Service Data is hosted if a Subscriber purchases the Data Center Location Add-On. A full description of this offering is provided at <https://support.zendesk.com/hc/en-us/articles/360053579674>

14. Availability and Continuity: Zendesk maintains a publicly available system-status webpage, which includes system availability details, scheduled maintenance, service incident history, and relevant security events, found at: https://status.zendesk.com/?_ga=2.228109981.1069242886.1631551570-1973870648.1630415696

Zendesk employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime and/or our Enhanced Disaster Recovery service offering allows us to deliver a high level of service availability, as Service Data is replicated across available zones. Our Disaster Recovery program ensures that our Services remain available and are easily recoverable in the case of a disaster, through building a robust technical environment. Additional details at:

https://support.zendesk.com/hc/en-us/articles/360022191434-Business-Continuity-and-Disaster-Recovery?_ga=2.57827498.1069242886.1631551570-1973870648.1630415696



15. People Security: Zendesk performs pre-employment background checks of all employees, including education and employment verification, in accordance with applicable local laws. Employees receive security training upon hire and annually thereafter. Employees are bound by written confidentiality agreements to maintain the confidentiality of data.

16. Vendor Management: Zendesk uses third party vendors to provide certain aspects of the Services. Zendesk completes a security risk assessment of prospective vendors.

17. Bug Bounty: Zendesk maintains a bug bounty program to allow independent security researchers to report security vulnerabilities on an ongoing basis, available at:

<https://support.zendesk.com/hc/en-us/articles/115002853607-Zendesk-Bug-Bounty-Program>

Zendesk Technical and Organisational Security Measures - Innovation Services

The full text of Zendesk's technical and organisational measures to protect Service Data for Enterprise Services is available at <https://www.zendesk.com/company/agreements-and-terms/protect-service-data-innovation-services/>. The Zendesk information security program includes documented policies or standards governing the handling of Service Data in compliance with applicable law, and administrative, technical and physical safeguards designed to protect the confidentiality and integrity of Service Data. Zendesk reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this document.

1. Physical Access Controls: Zendesk takes reasonable measures to prevent physical access to prevent unauthorised persons from gaining access to Service Data.

2. System Access Controls: Zendesk takes reasonable measures to prevent Service Data from being used without authorisation.

3. Data Access Controls: Zendesk takes reasonable measures to provide that Service Data is accessible and manageable only by properly authorised staff.

4. Transmission Controls: Zendesk takes reasonable measures to ensure the ability to check and establish to which entities the transfer of Service Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport.

5. Input Controls: Zendesk takes reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed; and, any transfer of Service Data to a third-party service provider is made via a secure transmission.

6. Logical Separation: Data from different Zendesk's subscriber environments is logically segregated on systems managed by Zendesk to ensure that Service Data that is collected by different data controllers is segregated from one another.

7. Security Policies and Personnel. Zendesk has and will maintain a managed security program to identify risks and implement preventative technology, as well as technology and processes for common attack mitigation. We have, and will maintain, a full-time information security team responsible for safeguarding our networks, systems and services, and developing and delivering training to our employees in compliance with our security policies.



ANNEX III

Sub-processors Security Standards for Enterprise Services

As of the Effective Date of this DPA, Our Sub-processors, when processing Service Data on behalf of Subscriber in connection with the Enterprise Services, shall implement and maintain the following technical and organisational security measures for the Processing of such Service Data (“**Enterprise Services Security Standards**”):

1. Physical Access Controls: Our Sub-processors will take reasonable measures, such as security personnel and secured buildings, to prevent unauthorised persons from gaining physical access to Service Data.

2. System Access Controls: Our Sub-processors will take reasonable measures to prevent Service Data from being used without authorisation. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorisation processes, documented change management processes and/or, logging of access on several levels.

3. Data Access Controls: Our Sub-processors will take reasonable measures to ensure that Service Data is accessible and manageable only by properly authorised staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to access Service Data only have access to Service Data to which they have privilege of access; and, that Service Data cannot be read, copied, modified or removed without authorisation in the course of processing. Vendor will implement and maintain an access policy under which access to its system environment, to data processing systems, to Service Data, and other data is restricted to authorised personnel only.

4. Transmission Controls: Our Sub-processors will take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Service Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport.

5. Input Controls: Our Sub-processors will take reasonable measures to ensure that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed; and, any transfer of Service Data to a third-party service provider is made via a secure transmission.

6. Data Protection: Our Sub-processors will take reasonable measures to ensure that Service Data is secured to protect against accidental destruction or loss. Our Sub-processors shall ensure that, when hosted by Sub-processor, backups are completed on a regular basis, are secured and encrypted, to ensure that Service Data is protected. Our Sub-processors will implement and maintain a managed security program to identify risks and implement preventative technology and processes for common attack mitigation.

7. Logical Separation: Our Sub-processors will logically segregate Service Data from the data of other parties on its systems to ensure that Service Data may be processed separately.