Zendesk's DPA

zendesk

DATA PROCESSING AGREEMENT

This Data Processing Agreement is entered into by EduTech / WFL BOCES ("**Subscriber**") and Zendesk, Inc. ("**Zendesk**"), each a "**Party**" and together the "**Parties**".

1. PURPOSE

1.1 Subscriber and Zendesk have entered into a Main Services Agreement ("**MSA**") pursuant to which Subscriber is provided access and use of 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 equivalent requirements in other Applicable Data Protection Law 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 for the specific purpose of providing the Service(s) to Subscriber, and 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 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 not:

(a) retain, use, or disclose Personal Data (i) for any purpose other than for the specific purpose of providing the Service(s) to Subscriber as set out in the MSA, this DPA, and other relevant agreement(s); (ii) outside of the direct business relationship between Zendesk and Subscriber; or (iii) as otherwise prohibited by Applicable Data Protection Law;

(b) Sell or Share Personal Data; or

(c) combine Personal Data that it receives from Subscriber with Personal Data it receives from, or on behalf of, another person, or collects from its own interactions with data subjects, except where both (i) expressly required to perform the Service(s) and (ii) permitted by Applicable Data Protection Law;

(iii) 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 and;

(iv) to notify Subscriber if it determines that it can no longer meet its obligations under Applicable Data Protection Law and allow Subscriber to take reasonable and appropriate steps to remediate unauthorised processing of Personal Data.

(v) 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**;

(vi) to notify Subscriber in accordance with Article 33(2) of the GDPR and equivalent requirements in other Applicable Data Protection Law, 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;

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

(viii) to assist Subscriber, taking into account the nature of the processing and insofar as it is commercially reasonable, to fulfill 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 Subscriber (to the extent Zendesk is able to associate the data subject with Subscriber). In the event Subscriber is unable to address the Data Subject Request, taking into account the nature of the processing and using information made available by Subscriber necessary to complete the Data Subject Request, 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 Applicable Data Protection Law;

(ix) upon request, 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;

(x) 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);

(xi) to comply with the requirements of Section 5 of this DPA (Audit); and

(xii) 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 Applicable Data Protection Law. 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://support.zendesk.com/hc/en-us/articles/4408883061530-Sub-processors ("**Sub-processor Policy**") in accordance with Article 28 of the GDPR and equivalent requirements in other Applicable Data Protection Law 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 with 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 Zendesk's Website.

zendesk

4.3 In the event that Subscriber objects to the processing of its Personal Data by any proposed Sub-processor as described in Section 4.2 on reasonable grounds relating to data protection, it shall inform Zendesk in writing by emailing privacy@zendesk.com within thirty (30) days following the update of the Sub-processor Policy above. In such event, the Parties shall negotiate in good faith a solution to Subscriber's objection. If the Parties cannot reach resolution within sixty (60) days of Zendesk's receipt of Subscriber's objection, Zendesk will either (a) instruct the Sub-processor to not process 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 and validate the level of compliance from which Zendesk provides its data processing services. These audits:

(i) will be performed at least annually;

(ii) will be performed according to requirements of the applicable International Standard(s) including ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), ISAE (International Standard for Assurance Engagements) 3402, SSAE (Statement on Standards for Attestation Engagements) 18, or such other alternative standards that are substantially equivalent to such frameworks;

(iii) will be performed by independent third-party security professionals at Zendesk's selection and expense; and

(iv) will result in the generation of certificate(s) and/or an audit report(s) affirming that Zendesk's data security controls achieve prevailing industry standards in accordance with attestation standards established by the International Standards Organization and/or the American Institute of Certified Public Accountants (AICPA) or such other alternative standards that are substantially equivalent ("**Report**").

5.2 At Subscriber's written request and without charge, Zendesk will provide Subscriber with a confidential summary of the Report ("**Summary Report**"). The Summary Report will constitute Zendesk's Confidential Information under the confidentiality provisions of Zendesk's MSA.

5.3 To the extent Subscriber's audit obligations under Applicable Data Protection Law are not reasonably satisfied through a Summary Report or other documentation Zendesk makes generally available to its Subscribers, Subscriber may request to conduct an audit of Zendesk under Applicable Data Protection Law ("**Data Protection Audit**") upon at least thirty (30) days' advance written notice to privacy@zendesk.com. Such Data Protection Audit shall be conducted no more than once during any twelve-month period and shall be conducted during normal business hours with reasonable duration, and not to interfere with Zendesk's operations. Subscriber may conduct such Data Protection Audit or may use an independent, accredited third-party audit firm subject to an appropriate duty of confidentiality with Zendesk. Subscriber acknowledges that Zendesk has a multi-tenant cloud environment and any on-site Data Protection Audit will be limited to the Zendesk corporate headquarters or mutually agreed upon regional main office. No Data Protection Audit shall involve access to any data relating to any other Zendesk subscriber or to systems or facilities not involved in the processing of Personal Data for Subscriber and in no event shall a Data Protection Audit cause Zendesk to violate its confidentiality obligations to any third party. Subscriber shall be responsible for all costs and expenses relating to a Data Protection Audit conducted under this Section 5.3, including for any time Zendesk expends on such audit at Zendesk's then-current professional services rates. Any report generated in connection with such a Data Protection Audit shall be considered Zendesk's Confidential Information and shall be promptly provided

to Zendesk. In the event of a conflict between the audit terms in this Section 5.3 and the audit terms in the EU SCCs and/or UK Addendum, the audits terms in the EU SCCs and/or UK Addendum shall control. Nothing in this Section 5.3 modifies or affects any supervisory authority's rights under the EU SCCs and/or UK Addendum.

6. INTERNATIONAL DATA EXPORTS

6.1 Subscriber acknowledges that if Zendesk and its Sub-processors process Personal Data subject to the GDPR, UK Data Protection Law, or FADP ("**European Data**"), Zendesk may process such 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 Zendesk processes European Data in a country that has not received an adequacy decision from the European Commission or Swiss or UK authorities, as applicable, such transfer shall take place on the basis of (i) the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**"), as applicable; (ii) the Zendesk Binding Corporate Rules as set out in Section 6.2; or (iii) the EU SCCs and/or UK Addendum, as applicable. 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 order listed in this Section. If the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. DPF is declared invalid, or if Zendesk fails to re-certify for the EU-U.S. DPF, then the transfer of Personal Data will be subject to the transfer mechanism listed in (ii) or (iii) of this Section. If neither (i), (ii) nor (iii) is applicable, the Parties agree to work in good faith without undue delay to implement an appropriate transfer mechanism authorised under Applicable Data Protection Law.

6.2 Binding Corporate Rules

Where Zendesk processes or permits any Sub-processor within the Processor Group to process European Data, Zendesk shall comply in full with the requirements of Zendesk's Binding Corporate Rules in order to provide adequate protections for the European Data that it processes on behalf of Subscriber, which are available at https://d1eipm3vz40hy0.cloudfront.net/pdf/Zendesk-BCR-Processor-Policy-2022.pdf

6.3 EU SCCs

Where Zendesk processes Personal Data that is subject to the GDPR in a country that has not received an adequacy decision from the EU Commission and if Section 6.2 (Binding Corporate Rules) does not apply, the Parties hereby incorporate the EU SCCs by reference.

Where the EU SCCs apply, they will be deemed 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.

(ii) in Clause 7, the optional docking clause will not apply;

(iii) in Clause 9(a), Option 2 "General Written Authorisation" 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 17, Option 1 will apply and will be governed by the laws provided in the MSA. If the MSA is not governed by an EEA member state law, then the laws of Ireland shall govern;

(vi) in Clause 18(b), disputes shall be resolved before the courts provided in the MSA. If the MSA does not provide courts in an EEA Member State, the parties agree to the courts of Dublin;

(vii) Annex I.A and I.B and Annex II of the EU SCCs shall be deemed completed with the information set out in **Annex I and Annex II** to this DPA; and

(viii) in Annex I.C of the EU SCCs, where the data exporter is established in the EEA shall be the Supervisory Authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer. Where the data exporter is not established in the EEA, but is within the territorial scope of application of GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1), the Supervisory Authority

shall be the member state in which the representative within the meaning of Article 27(1) is established. If the data exporter is not established in the EEA, but falls within the territorial scope of application of GDPR without having to appoint a representative pursuant to Article 27(2), the Supervisory Authority of Ireland shall act as the competent Supervisory Authority.

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 UK Addendum

When Zendesk processes Personal Data subject to UK Data Protection Law in a country that has not received an adequacy decision from the UK authorities, and if Section 6.2 (Binding Corporate Rules) does not apply, the Parties hereby incorporate the UK Addendum for Personal Data subject to UK Data Protection Law by this reference. Where the UK Addendum applies, it will be deemed completed as follows:

(i) Table 1 shall be deemed completed with the information set out in **Annex I** of this DPA, the contents of which are hereby agreed by the Parties;

(ii) Table 2, the Parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum", and the accompanying table shall be deemed completed according to the Parties' preferences outlined in Section 6.3 above;

(iii) Table 3, shall be deemed completed with the information set out in **Annex I and Annex II** and Section 4 of this DPA; and

(iv) Table 4, the Parties agree that neither Party may terminate the UK Addendum as set out in Section 19.

6.5 Switzerland under EU SCCs

Where Zendesk processes Personal Data subject to FADP in a country that has not received an adequacy decision from Swiss authorities, and if Section 6.2 (Binding Corporate Rules) does not apply, the Parties hereby incorporate the EU SCCs (for Personal Data subject to FADP) by this reference. To the extent Personal Data transfers are subject to FADP, the EU SCCs shall be deemed completed with the information set forth in Section 6.3 above, as appropriate, and the following shall apply:

The term "member state", as used in the EU SCCs, shall not be interpreted to limit data subjects in Switzerland from being able to sue for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs. Until the revised FADP comes into effect (the version enacted on 25 September 2020, as amended), the EU SCCs shall also protect the data of legal entities. For the purposes of Annex I.C of the EU SCCs, where Subscriber is the data exporter and the Personal Data transferred is exclusively subject to FADP, the Swiss Federal Data Protection and Information Commissioner (the "**FDPIC**") shall be the competent Supervisory Authority. Where the Personal Data transferred is subject to both the FADP and the GDPR: (i) parallel supervision should apply; or (ii) for the (revised) FADP, the FDPIC shall be the competent Supervisory Authority insofar as the transfer is governed by the (revised) FADP and for the GDPR, the competent Supervisory Authority is as determined in Section 6.3(viii). References to the GDPR should be understood as references to the FADP and, once effective, the (revised) FADP, insofar as Personal Data transfers are subject to the FADP or (revised) FADP.

6.6 Transfers to the US under the Data Privacy Framework.

Zendesk has certified to participate in and comply with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") (see: https://www.dataprivacyframework.gov/s/). Zendesk commits to maintain the self-certification of compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, or any replacement framework, for the Services provided under the Agreement and this DPA.

6.7 Brazil LGPD

The EU SCCs will be used for transfers to countries not deemed adequate per the LGPD. In Clause 17, Option 1 will apply, and will be governed by the laws of Brazil; (ii) in Clause 18(b), disputes shall be resolved before a court of general jurisdiction in São Paulo/SP, Brazil.

zendesk

6.8 Singapore PDPA

Where the PDPA applies, Zendesk's obligations to Subscriber under the DPA are those express obligations imposed by the PDPA on a "data intermediary" (processor) when processing personal data on behalf of "organisation" (controller). Notwithstanding Section 12.1, any claims arising from or related to the Singapore PDPA will be governed by the laws of Singapore and disputes shall be resolved before a court of general jurisdiction in Singapore.

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 Subscriber may export its Service Data before termination of Subscriber's access to the Service. Upon Subscriber's written request, Zendesk will make available to Subscriber the ability to export or download, as provided in the Documentation, its Service Data after termination subject to the terms set forth in the MSA. Upon termination or cancellation, Zendesk will delete Subscriber Service Data in accordance with Zendesk's Service Data Deletion Policy.

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 Affiliate arising out of or related to the MSA and this DPA shall apply in aggregate for all claims under both the MSA and this DPA. This section shall not be construed as limiting the liability of either Party with respect to claims brought by data subjects or under the EU SCCs' Clause 12 and/or the UK Addendum.

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 The governing law and jurisdiction will be governed by the MSA, unless otherwise stated herein.

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 Breach**", "**Sell**", "**Share**", "**processing**", "**process**", "**processor**", "**controller**", "**data exporter**", "**data importer**" and "**data subject**" shall have the same meaning as in and be inclusive of similar concepts under Applicable Data Protection Law and may be lowercase or capitalised herein.

13.1 Applicable Data Protection Law: means, in addition to the laws and regulations applicable to certain jurisdictions referred to in the Region-Specific Terms set out in the MSA, all data protection laws and regulations applicable to Zendesk in connection with Zendesk's processing of Personal Data as a Processor to provide the Service(s) to Subscriber, including LGPD and PDPA as applicable. Notwithstanding the foregoing, "Applicable Data Protection Law" excludes (a) laws requiring the localisation of Personal Data and (b) laws specific to Subscriber or Subscriber's industry that are not generally applicable to Zendesk as Processor.

zendesk

13.2 EU SCCs: means the standard contractual clauses for the transfer of Personal Data to Controllers and Processors established in third countries, adopted by the European Commission from time to time, the adopted version of which in force at the date of signature of this DPA is that set out in the Annex to the European Commission's Implementing Decision 2021/914 of 4 June 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914, and as may be amended or replaced from time to time.

13.3 EU-US Data Privacy Framework means the framework approved by the European Commission on July 10th, 2023, by adopting Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework.

13.4 FADP: means the Swiss Federal Act of 19 June 1992 on Data Protection (as may be amended or superseded) and related ordinances, and, once effective, the revised FADP version of 25 September 2020, as amended or replaced and applicable.

13.5 GDPR: means the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended from time to time, and any applicable national laws implemented by European Economic Area ("EEA") member states.

13.6 LGPD: means the Lei Geral de Proteção de Dados Pessoais, Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended).

13.7 PDPA: means the Personal Data Protection Act of 2012 of Singapore (as amended).

13.8 Personal Data: means any information relating, directly or indirectly, to an identified or identifiable natural person that is contained in Service Data and processed by Zendesk on behalf of Subscriber as a Processor under the MSA. Without limiting the generality of the foregoing, "Personal Data" includes but is not limited to "personal data," "personal information," and equivalent concepts under Applicable Data Protection Law to the extent such data is processed by Zendesk on behalf of Subscriber as a Processor under the MSA.

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

13.10 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 Main Services Agreement should be considered a reference to the Reseller Subscription Services Agreement for customers of Zendesk resellers.

13.11 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.

13.12 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.

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

13.14 UK Addendum: means the UK 'International Data Transfer Addendum to the EU Commission Standard Contractual Clauses', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

13.15 UK Data Protection Law: means the Data Protection Act (DPA 2018), as amended, and the GDPR as incorporated into UK law as the UK GDPR, as amended, and any other applicable UK data protection laws, or regulatory Code of Conduct or other guidance that may be issued from time to time.

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

13.17 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

zendesk

representatives as of the last date of execution below ("**Effective Date**").

Subscriber: EduTech / WFL BOCES	**Zendesk**
BY: Kelli Eckdahl	BY: DocuSigned by: James Fash BFA91564AAD2434...
NAME: Kelli Eckdahl	NAME: James Fash
TITLE: Director	TITLE: VP & AGC, Commercial Legal
DATE: 3/19/24	DATE: December 4, 2023
EMAIL: Kelli.Eckdahl@wflboces.org	EMAIL: privacy@zendesk.com

APPROVED FOR SIGNATURE zendesk ZENDESK LEGAL DEPARTMENT

zendesk

ANNEX I
Details of Processing

Data Exporter: Subscriber
Contact Details: Provided in the DPA signature block.
Data Exporter Role: Subscriber is EduTech / WFL BOCES

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). "Sensitive Data" shall have the same meaning as special categories of personal data in Article 9 of the GDPR and be inclusive of similar concepts under Applicable Data Protection Law.

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

zendesk

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/trust-center/ 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 validates third parties operating data centers on Zendesk's 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 are transferred Service Data by means of data transmission facilities 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 that 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 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.

zendesk

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. Zendesk's network security architecture consists of multiple zones with more sensitive systems, like database servers, in Zendesk's 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. Zendesk's 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 Zendesk's 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 Zendesk's Enhanced Disaster Recovery service offering allows us to deliver a high level of service availability, as Service Data is replicated across available zones. Zendesk's Disaster Recovery program ensures that Zendesk's 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 Innovation Services is available at https://www.zendesk.com/company/agreements-and-terms/protect-service-data-innovation-services/.

zendesk

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 unauthorised persons from gaining physical 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 are transferred Service Data by means of data transmission facilities 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 that 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 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 Zendesk's networks, systems and services, and developing and delivering training to Zendesk's employees in compliance with Zendesk's security policies.

zendesk

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.