

ADA DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is made as of the date of the applicable Services Agreement or Terms of Use (the “**Main Agreement**”), which incorporates this DPA, between Ada Support Inc. (“**Supplier**”) and the customer entity identified in the Main Agreement (the “**Customer**”). Together Supplier and Customer are the “**Parties**”.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Main Agreement solely to the extent that Supplier Processes Personal Data belonging to Customer.

Except where the context requires otherwise, references in this DPA to the Main Agreement are to the Main Agreement as amended by, and including, this DPA. Capitalized terms used and not otherwise defined herein have the meanings given to them in the Data Protection Laws or the Main Agreement.

1. DEFINITIONS

- 1.1 “**CCPA**”: means the California Consumer Privacy Act of 2018, codified at California Civil Code Title 1.81.5, Section 1798.100 et seq., and any associated regulations and amendments thereto, including, the California Privacy Rights Act amendments (“**CCPA**”).
- 1.2 “**Customer Content**”: means any data, file attachments, text, images, reports, personal information, or other content that is uploaded or submitted to the Services by Customer or Customer’s users and is processed by Supplier on behalf of Customer. For the avoidance of doubt, Customer Content does not include aggregated or deidentified information, or other usage, statistical, or technical information generated by the Services for Supplier’s internal business purposes.
- 1.3 “**Data Controller**”: has the meaning set out in the Data Protection Laws and shall include the term "Business" as defined in the CCPA.
- 1.4 “**Data Processor**” (which shall also include the term "Service Provider"), “**Processing**” and “**Process**” have the meaning set out in the Data Protection Laws.
- 1.5 “**Data Protection Addendum**” or “**DPA**” or “**Addendum**” means this Data Processing Addendum, including any and all subsequent amendments thereto, comprising the terms and conditions in the main body of this document, together with the schedules,

the annexes and any attachments, and any documents expressly incorporated by reference;

- 1.6 **“Data Protection Laws”**: means any data protection laws applicable to Supplier’s Processing of Personal Data as contemplated by the Main Agreement including, without limitation, in particular (a) the European Union General Data Protection Regulation 2016/679 (**“GDPR”**), UK Data Protection Act of 2018 (**“UK GDPR”**), Swiss Federal Act on Data Protection (**“FADP”**), and any related decisions or guidelines and subsequent legislation of a similar nature, and all privacy, security, and legally-binding data protection laws and rules, (b) the CCPA, as it may be amended from time to time, and (c) similar laws governing data protection in any applicable jurisdiction in which the Services are being provided or Personal Data is being Processed and any jurisdiction from which the Supplier or any Subprocessor provides any of the Services or from which the Customer provides its products or services.
- 1.7 **“Data Subject”**: means an individual about whom the Personal Data relates.
- 1.8 **“EEA”**: means, for purposes of this DPA, the European Economic Area, the United Kingdom, and Switzerland.
- 1.9 **“Personal Data”**: means Customer Content that directly or indirectly identifies or relates to an identifiable Data Subject.
- 1.10 **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Supplier pursuant to the Main Agreement and this DPA.
- 1.11 **“Services”**: means the services to be provided by Supplier to Customer as set out in the Main Agreement.
- 1.12 **“Subprocessor”**: means any third party, but excluding an employee or consultant of the Supplier or any of its sub-contractors, appointed by or on behalf of the Supplier to Process Personal Data on behalf of Supplier to assist in providing Services to the Customer in connection with the Main Agreement.

2. CONTINUITY

2.1 Terms used in this DPA shall have the same meaning as defined in the Main Agreement, unless defined differently herein.

3. PURPOSE AND SCOPE

3.1 The terms of this DPA will apply in the place of any data protection clauses included in Ada's Privacy Policy or Main Agreement with respect to Supplier's Processing of Personal Data on behalf of Customer in order to provide Services. If the Supplier Processes any Personal Data on the Customer's behalf when performing its obligations under the Main Agreement, the parties agree that the Customer shall be the Data Controller and the Supplier shall be the Data Processor.

3.2 Notwithstanding anything in this DPA, any obligation of Supplier under this DPA shall be interpreted to require Supplier to perform only what is reasonably required to allow the Customer to meet its obligations under applicable Data Protection Laws.

4. PERSONAL DATA

4.1 Through the Customer's use of the Services, the Customer decides what data to collect from its end users and how to use the information Processed via the Services.

4.2 The Customer warrants to the Supplier that it is entitled to transfer the relevant Personal Data to the Supplier and that the Supplier is entitled to transfer relevant Personal Data to its Subprocessors and third-party providers so that the Supplier may lawfully use, Process and transfer the Personal Data in accordance with the Main Agreement and this DPA on the Data Controller's behalf.

5. DETAILS OF THE PROCESSING CONTEMPLATED UNDER THIS DPA

5.1 Details of the Processing contemplated under this DPA are set out in Annex 1.

5.2 The Supplier may provide notice of change to these provisions where an update is required due to changes to the Services or changes required due to applicable Data Protection Laws.

6. PERMITTED PROCESSING AND DISCLOSURE OF PERSONAL DATA

- 6.1 The Supplier must, and shall procure that its Subprocessors shall, Process any Personal Data held in connection with Main Agreement only for the purposes of fulfilling its obligations under Main Agreement, as permitted by applicable Data Protection Laws, and in accordance with relevant documented instructions of the Customer (unless required to do so by a relevant Data Protection Law to which the Supplier is subject; in such a case the Supplier shall inform the Data Controller of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest). The Customer agrees to provide the Supplier with clear documented instructions relating to Personal Data under this Agreement.
- 6.2 In connection with its Processing of Personal Data as described in this DPA and the Main Agreement, Supplier shall not (a) "sell" or "share" any Personal Data, as such terms are defined in the CCPA and similar Data Protection Laws; (b) retain, use or disclose Personal Data for a commercial purpose other than providing the Services as provided in the Main Agreement and this DPA, or as otherwise permitted by applicable Data Protection Laws; (c) attempt to link, identify, or otherwise create a relationship between Personal Data and non-personal data or any other data without Customer's express authorization; and (d) Supplier certifies that it understands and will comply with the restrictions described in this Clause 6 and that it will provide the same level of protection for the Personal Data subject to the CCPA as is required under the CCPA
- 6.3 The Supplier agrees to make reasonable efforts to assist the Customer in ensuring compliance with its obligations under applicable Data Protection Laws, where required, including the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the Processing and the information available to the Supplier, and in accordance with Clause 16.

7. DATA SUBJECT RIGHTS

- 7.1 Supplier will, to the extent legally permitted, promptly notify Customer or refer the Data Subject to Customer for handling if Supplier receives any requests from a Data Subject seeking to exercise any rights afforded to them under Data Protection Laws regarding their Personal Data (each, a "**Data Subject Request**"). Supplier will not

respond to such Data Subject Requests itself, and Customer authorizes Supplier to redirect the Data Subject Request as necessary to Customer for handling.

- 7.2 In the event Customer is unable to address a Data Subject Request through the Services' self-service capabilities, Supplier will, upon Customer's request, provide commercially reasonable assistance to assist Customer in responding to the Data Subject Request, to the extent Supplier is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer will be responsible for any costs arising from Supplier's provision of this additional support to assist Customer with a Data Subject Request.

8. SECURITY AND INTEGRITY OF PERSONAL DATA

- 8.1 The Supplier agrees to take technical and organisational measures set forth in the applicable DPA Annex 2 designed to provide a level of security appropriate to the risk for Supplier's scope of responsibility and the Personal Data Processed. The technical and organisational measures are subject to technical progress and development. Supplier reserves the right to modify the technical and organisational measures provided that the functionality and security of the Services are not degraded and that all such measures remain at least as robust as those in Annex 2. Customer confirms that the technical and organisational measures provide an appropriate level of protection for the Customer Personal Data taking into account the risks for Supplier's Processing of Personal Data.

- 8.2 The Supplier shall, and shall procure that its Subprocessors shall, take all reasonable steps to ensure that Personal Data Processed in connection with Main Agreement is Processed in compliance with the obligations under Article 32 of the GDPR, Section 1798.150(a) of the CCPA, and similar requirements in applicable Data Protection Laws, to the extent applicable in the relevant context, relating to security of Processing.

9. PERSONAL DATA BREACH NOTIFICATION.

- 9.1 Supplier will notify Customer without undue delay after becoming aware of a Personal Data Breach. The Supplier will also reasonably cooperate with the Customer with respect to any investigations and with preparing legally required notices, and provide any information reasonably requested by the Customer in

relation to the Personal Data Breach, provided such information does not constitute proprietary or trade secret information of Supplier.

10. AUDITS

10.1 The Supplier will make available to the Customer all information necessary to demonstrate compliance with the data Processing obligations laid down in this DPA including by allowing for and contributing to reasonable audits to determine the Supplier's compliance with its obligations under this DPA in accordance with the following procedures:

- (a) upon Customer's written request, Supplier will provide Customer with its most recent summary audit report pertaining to Supplier's Processing of Personal Data and compliance with applicable Data Protection Laws.
- (b) if required by Customer, Supplier will provide reasonable cooperation to Customer by providing further information regarding its technical and organisational measures or other information pertaining to Supplier's Processing of Personal Data contained in the audit report.
- (c) to the extent it is not possible to otherwise satisfy an audit obligation required by applicable law, Customer or Customer's mandated auditor may perform an audit of Supplier's relevant documents and systems used to provide the Service subject to arranging a mutually agreeable time and provided that each audit is carried out at the Customer's cost, during normal business hours, so as to cause the minimum disruption to the Supplier's business, subject to the Customer and its auditors (if relevant) undertaking reasonable and appropriate confidentiality obligations.

10.2 The scope of an audit will be limited to the Supplier's systems, Processes and documentation relevant to the Processing and protection of Personal Data Processed in the provision of the Services and the Customer or its auditor will not have any access to any data belonging to a person other than the Customer. Customer shall be entitled to audit Supplier no more than once per year, unless otherwise required by applicable law.

- 10.3 The Supplier shall inform the Customer if, in the Supplier's reasonable opinion, an instruction given by the Customer under Clause 6.1 infringes the Data Protection Laws. This opinion shall not be construed by the Customer as legal advice.
- 10.4 For purposes of compliance with the CCPA, the parties agree that Customer has the right to take reasonable and appropriate steps to (a) ensure that Supplier is Processing Personal Data consistent with applicable Data Protection Law and (b) stop and remediate unauthorized use of Personal Data.

11. CONFIDENTIALITY

- 11.1 The Supplier shall, and shall procure that its Subprocessors shall, ensure that any persons to whom the Supplier discloses Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality with respect to the Personal Data.

12. APPOINTMENT OF SUBPROCESSORS

- 12.1 The Supplier uses Supplier Subprocessors to provide services including, but not limited to centralized logging, database hosting, error reporting, and cloud computing. These Supplier Subprocessors will have access to the data Processed via the Services, including relevant Personal Data. These Subprocessors are only permitted to Process this data for the purposes of providing their specifically contracted services to the Supplier.
- 12.2 With respect to each Subprocessor, the Supplier shall ensure that it has entered into a written agreement that contains data protection terms with respect to Processing of the Personal Data that are consistent with the requirements in this DPA. For the avoidance of doubt, the Supplier shall be liable for the acts and omissions of its Subprocessors to the same extent the Supplier would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Main Agreement.
- 12.3 The Customer provides a general authorisation to the Supplier to engage the Subprocessors listed at www.ada.cx/subprocessors as are appointed on the date this DPA came into force, as well as any Supplier affiliates.
- 12.4 The Supplier:

- (a) Has provided to the Customer a list of all Subprocessors who are involved in Processing or subprocessing Personal Data in connection with the provision of the Services; and
 - (b) Will provide the Customer with additional information about any Subprocessor on the Subprocessor List that the Customer may reasonably require to comply with Data Protection Laws.
- 12.5 The Supplier will inform the Customer of any intended changes concerning the addition or replacement of Subprocessors, thereby giving the Customer the opportunity to object to such changes. The Customer may object to any such addition or replacement of Subprocessors within ten (10) business days of such notice, provided such objection is in writing and based on reasonable grounds relating to data protection. If the Customer objects to such a change the objection will be referred to dispute resolution. If the Supplier fails to provide a reasonable solution to resolve the dispute within ninety (90) days, the Customer will be entitled to terminate the affected Services by giving not less than ninety (90) days' written notice to that effect to the Supplier.

13. TRANSFERS OF PERSONAL DATA OUTSIDE EUROPEAN ECONOMIC AREA

- 13.1 As the Supplier operates globally, the Customer hereby approves the transfer and Processing of Personal Data outside of the EEA in accordance with applicable Data Protection Laws, in connection with the Agreement.
- 13.2 The European Commission ("**EC**"), pursuant to Article 45 of Regulation 2016/679, the United Kingdom Information Commissioner's Office ("**ICO**"), and the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"), have issued adequacy decisions in respect of Canadian commercial organisations. As a result of these decisions, the transfer of Personal Data to Canada, in connection with the Agreement, is subject to an adequate level of protection, in compliance with Data Protection Laws, and Customer agrees that no additional transfer mechanism is required for transfers of Personal Data to Canada.
- 13.3 In the event that the EC, UK ICO, and/or FDPIC no longer recognize Canada as an "adequate" jurisdiction for data transfers, or in the event that the Services change to result in a direct transfer of Personal Data to jurisdictions outside of Canada that do not maintain an adequacy determination, Supplier and Customer agree that the Standard Contractual Clauses issued pursuant to Commission Implementing

Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, located http://data.europa.eu/eli/dec_impl/2021/914/oj. (the "**EU SCCs**"), govern such transfer and will be deemed signed and completed as follows:

- (a) With respect to Personal Data transfers for which the GDPR governs the international nature of the transfer, the parties agree that the EU SCCs apply and shall be completed as follows:
 - (i) Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a controller) to Supplier (as a Processor) and Module 3 applies to transfers of Personal Data from Customer (as a Processor) to Supplier (as a Subprocessor);
 - (ii) Clause 7 (the optional docking clause) is not included;
 - (iii) Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of Subprocessors and rules governing the appointment of such Subprocessors is as set out above in Clause 12;
 - (iv) Under Clause 11 (Redress), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;
 - (v) Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the law of Ireland;
 - (vi) Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;
 - (vii) Annexes I(A) and I(B) are completed as set forth in Annex 1 of this DPA;
 - (viii) Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission;
 - (ix) Annex II (Technical and organizational measures) is completed with Annex 2 of this DPA; and

- (x) Annex III (List of Subprocessors) is not applicable as the Parties have chosen General Authorization under EU SCCs Clause 9.
- (b) With respect to Personal Data transfers for which the UK GDPR governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>) (“UK SCCs”) forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:
 - (i) Table 1 of the UK SCCs: The Parties’ details shall be the Parties and their affiliates to the extent any of them is involved in such transfer. The Key Contact shall be the contacts set forth in the Main Agreement;
 - (ii) Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties pursuant to Clause 13.3 above;
 - (iii) Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Annexes 1 and 2 below; and
 - (iv) Table 4 of the UK SCCs: Either Party may end this DPA as set out in Section 19 of the UK SCCs.
- (c) For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Clause 13.3(a) of this Addendum, but with the following differences to the extent required by the FADP: (i) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (ii) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (iii) term “member state” in EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; and (iv) the relevant supervisory authority is the Swiss

Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

- (d) Supplier represents and warrants that any onward transfers of Personal Data to Subprocessors located in a jurisdiction outside of the EEA or a jurisdiction without an adequacy determination shall be made through binding EU SCCs in accordance with this Clause 13.3, or otherwise in accordance with applicable law.

13.4 In approving the transfer of personal data outside the EEA, under this Clause 13, the Customer confirms that the Customer will indemnify and hold harmless the Supplier (and its respective employees, directors, officers, shareholders lawyers, agents and representatives) from and against any and all claims, costs, losses, damages, judgments, penalties, interest and expenses (including reasonable legal fees and costs) arising out of any claim, action, audit, investigation, regulatory action, inquiry or other proceeding that arises out of or relates to the Customer's failure to comply with any applicable laws and regulations in connection with the transfer of the Personal Data outside the EEA, including any applicable data protection legislation. This indemnification obligation set forth herein shall survive the termination of this DPA.

14. RETURN OF PERSONAL DATA

14.1 Upon Customer's written request within 90 days of termination of the Main Agreement, Supplier will and shall procure that its Subprocessors shall at the Customer's election, unless a law binding on the Supplier or its Subprocessors prevents it from doing as requested:

- (a) return all the Personal Data to the Customer; or
- (b) destroy all the Personal Data, in a manner agreed to by the Customer.

14.2 The Supplier and its Subprocessors may retain Personal Data to the extent required by applicable Data Protection Laws and only to the extent and for such period as required by applicable Data Protection Laws and always provided that the Supplier shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified Main

Agreement or in the applicable Data Protection Laws requiring its storage and for no other purpose.

15. OBLIGATIONS INDEPENDENT OF OTHER PROVISIONS

15.1 The obligations contained in this DPA are without prejudice to the Supplier's and/or Subprocessors other obligations under the Main Agreement and apply notwithstanding any permitted use or disclosure of confidential information in this DPA.

16. COSTS

16.1 The costs of the Supplier and its Subprocessors to comply with their respective obligations as Processors under Data Protection Laws applicable in a specific jurisdiction shall be borne by the Supplier and its Subprocessors to the extent compliance with such obligations is necessary for the Supplier and/or its Subprocessors' compliance with applicable Data Protection Laws in their role as Processors in the jurisdiction in question.

16.2 Notwithstanding Clause 16.1 if the Supplier is requested by the Customer to take on compliance activities which go beyond the activities that the Supplier is required to do as a Data Processor under applicable Data Protection Laws, the Supplier shall be entitled to its reasonable costs.

16.3 Should changes to applicable Data Protection Laws, including the interpretation thereof, entail increased costs for the Supplier or its Subprocessors, the Supplier may, subject to providing written notice to the Customer, increase the rates charged to the Customer to reflect the increased costs.

17. ORDER OF PRECEDENCE

17.1 With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Main Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

18. SEVERANCE

18.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

19. GOVERNING LAW

19.1 The parties to (a) this DPA hereby submit to the choice of jurisdiction stipulated in the Main Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and (b) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Main Agreement.

DPA Last Updated: July 20, 2023

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

1. *The relevant parties are:* Customer and Supplier, with contact details and signatures as provided for each party in the Main Agreement.
2. *The subject matter of the Processing is:* The performance of the Main Agreement by the Supplier, pursuant to the Main Agreement.
3. *The duration of the Processing:* The Processing will continue until the expiration or termination of the Main Agreement.
4. *Nature and purpose of the Processing:* The Processing is carried out by the Supplier for the purposes of fulfilling its obligations under the Main Agreement and as further instructed in writing by the Customer.

5. *The types of Personal Data:*

In respect of end users, the types of personal data Processed may include details of end users' accounts with the Customer including username; password; email address; phone number; address; IP address; location; transcripts of conversations which take place using the Supplier's service and any other information which may be disclosed at the discretion of the end user when making a customer support query using the Supplier's service. In addition, the nature of the Services does not impose a technical restriction on the categories of Personal Data that may be Processed and therefore other categories of Personal Data may be included.

In respect of the Customer, the types of personal data Processed may include contact name; business address; email address; phone number; username; password; and basic site information i.e. URL/Channel/Impression Traffic etc.

6. *The categories of Data Subjects are:* Employees/contractors of the Customer and end users/customers of the Customer.

7. *The frequency of the transfer:* Continuous.

8. *The types of Sensitive Personal Data:* N/A. However, the nature of the Services does not impose a technical restriction on the categories of Personal Data that may be Processed.

ANNEX 2: Ada Support Security Overview

The current Security Overview can be found here <https://www.ada.cx/security>. This Security Overview describes Ada Support's security program, security certifications, technical, and organizational security controls to protect our services and customer data from unauthorized use, access, disclosure, or theft.

As security threats are constantly evolving, Ada reserves the right to update this Security Overview from time to time, provided, however, any update will not materially reduce the overall protections set forth in this Security Overview.