Data Processing Agreement

Version date: 23. September 2026

This Data Processing Agreement, including its Annexes, ("DPA") forms part of the Agreement between boost.ai and Customer for the purchase of Services (as defined in the Agreement. This DPA applies only where Customer has purchased Services directly from boost.ai, and does not apply where Services are purchased through a partner.

1. Purpose and Scope

1.1. This DPA governs the processing of Personal Data in the course of the provision of the Services provided by boost.ai or its Affiliates to the Customer and forms part of the Agreement between the Parties. This DPA regulates the Customer's rights and obligations in its capacity as data controller or processor as well as boost.ai's rights and obligations in its capacity as data processor when boost.ai processes Personal Data on behalf of the Customer under the Agreement. Another role distribution might follow from the situation or specific provisions in this DPA.

1.2. The purpose of this DPA is to ensure compliance with the requirements of Data Protection Laws on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.3. This DPA applies to the processing of personal data as specified in Annex II.

1.4. Annexes I to II of this DPA are an integral part of this DPA.

1.5. This DPA is without prejudice to obligations to which the Customer is subject by virtue of Data Protection Laws.

2. Defined Terms

Terms used in this DPA shall have the meaning as set forth below. Terms used in this DPA that are not defined below shall have the same meaning as given in the Agreement or the Data Protection Laws which they stem from, and shall be interpreted to include corresponding concepts under applicable Data Protection Laws.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 *et seq*., as amended by the California Privacy Rights Act, and its implementing regulations.

"**controller**" means the entity which determines the purposes and means of the processing of personal data, including as applicable ´business´ as that term is defined by the CCPA.

"**Data Protection Laws**" means all laws and regulations applicable to the processing of personal data under the Agreement, including those of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom, including the provisions of GDPR, the UK GDPR and Data Protection Act 2018, the California Consumer Privacy Act (CCPA), the Swiss Federal Act on Data Protection (nFADP), and other relevant regional data protection laws as amended from time to time, all only in so far as the requirements are directly applicable to boost.ai´s provision of the Services to Customer under the Agreement.

"**data subject**" means the identified or identifiable natural person to whom personal data relates, including as applicable "consumer" as that term is defined by the CCPA.

"**European personal data**" means the personal data subject to GDPR and any other European Data Protection Laws.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, including as implemented or adopted under the laws of the United Kingdom ("UK GDPR").

"**personal data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person,

"**processing**" and/or "**process**" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restrictions, erasure or destruction.

"**processor**" means the entity which processes personal data on behalf of the controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**sensitive personal data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses.

"**standard contractual clauses**" means the pre-approved model data protection clauses for the transfer of personal data to third countries pursuant to GDPR and approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"**sub-processo**r" means any processor engaged by the processor.

"**third-country transfer**" means a transfer of European personal data, including by way of remote access or onward transfer, to a recipient located in a country outside the European Economic Area ("EEA").

"**third-party auditor**" means a third-party independent contractor that is not a competitor of boost.ai that controller appoints to carry out any on-site audit.

3. Hierarchy

3.1. In the event of a contradiction between this DPA and the provisions of other parts of the Agreement, this DPA shall prevail with regard to processing of personal data by boost.ai. For the avoidance of doubt, this DPA shall prevail over any agreement regulating the processing of personal data that was entered into prior to the Effective Date.

4. Description of the Processing

4.1. The details of the processing operations, such as the categories of personal data, categories of data subjects, the duration of processing and the nature and purposes for which the personal data is processed on behalf of the controller, are specified in Annex II.

5. Obligations of the Parties

5.1. The processor shall process personal data only on documented instructions from the controller, unless the processor is otherwise required to do so in accordance with a legal requirement to which it is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless law prohibits this on important grounds of public interest.

5.2. The Parties agree that this DPA, the Agreement and the settings enabled by the controller, including the security and privacy settings adjusted by the controller directly in the Admin Panel, shall constitute the controller's documented instructions regarding processing of the personal data. Subsequent instructions may also be given throughout the duration of the processing of personal data. These instructions shall always be documented.

5.3. The controller acknowledges that settings are managed directly in the Admin Panel by users authorized by the controller and acting on controller's behalf. The controller is solely responsible for the adjustment of the settings and any adjustment of settings will be regarded as documented instructions to the processor regarding the processing of personal data, and may be automatically executed as such.

5.4. The processor shall immediately inform the controller if, in its opinion, instructions given by the controller infringe Data Protection Laws.

5.5. The controller is responsible for ensuring that the processing of personal data takes place in compliance with Data Protection Laws and this DPA. This also includes the obligations towards data-subjects, such as disclosing relevant information about the processing and other rights under Data Protection Laws which apply to the controller. The controller shall have sole responsibility for the accuracy, quality, and legality of personal data and the means by which controller acquired personal data.

6. Security of the processing

6.1. The processor shall implement and maintain appropriate technical and organizational measures to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the processor shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of

processing and the risks involved for the data subjects. The current specific technical and organizational measures implemented are published and maintained in the processor's Trust Center. In accordance with the stipulated assessment of the appropriate level of security, the processor may update these technical and organizational measures from time to time, provided that such updates maintain a level of security appropriate to the risk.

6.2. The controller is responsible for assessing that the security level provided by the processor through these technical and organizational measures are appropriate for the requirements following from the specific Data Protection Law, use case and risks associated with the personal data being processed.

6.3. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent necessary for the purposes described in Annex II and the Agreement.

6.4. The processor shall ensure that persons with access to personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received appropriate training on their responsibilities.

7. Sensitive Personal Data

7.1. No sensitive data is required to provide the Services. However, due to the nature of the Services and the possibility of processing open text, sensitive personal data may be processed if provided by the controller or their end users in its use of the Services or otherwise.

7.2. If the processing involves sensitive personal data, the controller shall manage the privacy and security settings in the Admin Panel in accordance with the risk. In addition to the general security measures maintained by the processor as set forth in Section 6 of this DPA, the processor provides additional privacy and security features which are configurable by the controller in the Admin Panel. The controller is solely responsible for adjusting these features as needed to ensure that the processing complies with Data Protection Laws which apply to it as controller and meets the security requirements associated with processing of sensitive personal data. The Parties agree that the processor's maintenance of the security measures set forth in Section 6, together with the provision of these additional configurable features, constitutes the processor's fulfillment of its obligation to implement safeguards appropriate for the processing of sensitive personal data.

8. Documentation and Audits

8.1. The Parties shall be able to reasonably demonstrate compliance with this DPA.

8.2. Upon controller´s written request, and subject to the confidentiality obligations set forth in the Agreement, the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from Data Protection Laws.

8.3. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this DPA.

8.4. Where Data Protection Law grants the controller a right to conduct audits, the processor shall allow for and contribute to audits, including on site inspections, conducted by the controller or another third-party auditor mandated by the controller. The practical arrangements for how and when such audits and inspections are requested, scheduled and carried out, including applicable notice periods, scope, and procedures, are set out in Annex I.

8.5. The Parties shall make the information referred to in this DPA, including the results of any audits, available to the competent supervisory authority/ies on request.

9. Use of sub-processors

9.1. The controller gives a general authorization to the processor for the engagement of sub-processors from the agreed list made available here https://trustcenter.boost.ai/subprocessors.

9.2. The processor shall, through the mechanism described in Annex 1, inform the controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

9.3. The mechanism for receiving notifications subject to section 9.2 is described in Annex I. The controller is responsible for ensuring that the recipient details are correct and keeping the recipient details updated.

9.4. Subject to Section 9.2 above, in the event that the controller objects to a new sub-processor, the Parties agree to discuss commercially reasonable alternative solutions in good faith. If the Parties cannot reach a resolution within ninety (90) days

from the date of controller's written objection, the controller may discontinue the use of the affected parts of the Services by terminating the affected parts of the Agreement. If no objection has been raised prior to processor replacing or appointing a new sub-processor, processor will deem controller to have authorized the new sub-processor.

9.5. Where the processor engages a sub-processor for carrying out specific processing activities on behalf of the controller, it shall do so by way of a contract which imposes on the sub-processor, in substance, data protection obligations no less protective than those imposed on the processor in accordance with this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The specific measures or activities chosen to fulfil an obligation may vary as long as the measures or activities chosen are appropriate and sufficient having regard to the nature, scope, context and purpose of the processing activities delegated to that sub-processor and the risks to the rights and freedoms of data subjects associated with those activities. The processor shall ensure that the sub-processor complies with the imposed data protection obligations.

9.6. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secrets or other confidential information, the processor may redact the text of the agreement prior to sharing the copy.

9.7. Unless otherwise set forth in the Agreement, where the sub-processor fails to fulfil its data protection obligations referred to in section 9.5, the processor shall remain fully responsible to the controller for the performance of the sub-processor's data protection obligations in accordance with this DPA.

10. International Data Transfer

10.1. Any Third-Country Transfer by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Data Protection Laws to which the processor is subject and shall take place using transfer mechanisms in compliance with the applicable Data Protection Laws.

10.2. The appointment of sub-processors located in third countries, as specified in the agreed list referenced in section 9.1, is deemed a documented instruction from the controller for the transfer of personal data to a third country.

10.3. Any Third-Country Transfer shall, where possible, rely on an applicable adequacy decision. The controller authorizes the processor to rely on the appropriate form of standard contractual clauses under Data Protection Law where such a Third-Country Transfer is not covered by an adequacy decision.

10.4. The specific transfer mechanisms for each identified transfer case are stipulated in Annex I.

11. Assistance to the controller

11.1. Processor provides controllers with a number of self-service features via the Admin Panel, including the ability to delete, obtain a copy of, or restrict use of data subjects' data. The controller may use such self-service features to assist in complying with its obligations under Data Protection Laws to which it is subject with respect to responding to data subject requests at no additional cost. To the extent controller does not have the ability to resolve a data subject's request through self-service features made available via the Admin Panel the processor will, upon controller's request, provide reasonable additional assistance to controller in complying with controller's data protection obligations with respect to data subject rights under Data Protection Laws to which controller is subject.

11.2. The processor shall promptly notify the controller of any request it has received from the data subject. The processor shall not respond to the request itself, unless authorized to do so by the controller.

11.3. In addition to the processor's obligation to assist the controller pursuant to this section, the processor shall furthermore provide controller with reasonable cooperation and assistance, taking into account the nature of the data processing and the information available to the processor, needed to fulfil the following obligations to the extent the controller is subject to these under Data Protection Laws. and:

11.3.1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') related to controller's use of the Services where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

11.3.2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the

processing related to controller's use of the Services would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

11.3.3. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

12. Notification of personal data breach

12.1. In the event of a personal data breach, the processor shall reasonably cooperate with and assist the controller to comply with obligations under Data Protection Laws to which controller is subject, taking into account the nature of processing and the information available to the processor.

12.2. In the event of a personal data breach concerning personal data processed by the processor on behalf of the controller in connection with the Services provided to controller under the Agreement, the processor shall, where required to assist with personal data breaches under Data Protection Laws, notify the controller without undue delay, and in any event, within seventy two (72) hours after having become aware of the breach.

12.3. The mechanism for receiving notifications subject to section 12.2 is described in Annex I. The controller is responsible for ensuring that the recipient details are disclosed and correct and keeping the recipient details updated.

12.4. Notification as referred to in section 12.2 shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

13. Non-compliance with the DPA and termination

13.1. Without prejudice to any obligations or rights under Data Protection Laws, in the event that the processor is in breach of its data protection obligations under this DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this DPA or the Agreement is terminated. The controller accepts that such suspension may result in the non-provision of the Services under the Agreement for the duration of the suspension without penalty to the processor. The processor shall inform the controller in case it is unable to comply with this DPA to the extent required under Data Protection Laws.

13.2. The processor shall be entitled to terminate the Agreement insofar as it concerns processing of personal data under this DPA where, after having informed the controller that the controller's instructions infringe applicable legal requirements in accordance with section 5.4, the controller insists on compliance with the instructions.

13.3. Following termination of the Agreement, the processor shall, at the choice of the controller, delete all remaining personal data processed on behalf of the controller and certify to the controller that it has done so, or return all the personal data to the controller and delete existing copies unless applicable Data Protection Laws or other laws to which the processor is subject require storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with this DPA.

14. Updates to this DPA

14.1. The version of this DPA published by the Processor as of the Effective Date shall apply. The Processor may not amend this DPA without the controller's prior written consent.

14.2. The Processor may update Annex I from time to time by giving the Controller at least 30 days' prior written notice, using the notification mechanism set out in Annex I. The Controller is responsible for ensuring that its recipient details are disclosed, correct and for keeping them up to date at all times.

15. Liability

15.1. The Parties agree to bear their own costs resulting from compensation and fines imposed directly upon such Parties in accordance with the Data Protection Laws to which each is subject. This is without prejudice to the principle of joint and several

liability towards the data subject pursuant to Data Protection Laws, in which case the right to claim back compensation (recourse) from the responsible Party shall apply in accordance with the Data Protection Laws, notwithstanding the limitation of liability set out in section 15.2.

15.2. The limitation of liability established by the Agreement shall apply to this DPA.

16. Applicable Law and Disputes

This DPA shall be governed and construed under the same laws and place of jurisdiction as that established by the Agreement.

ANNEX I

A. Audits

Compliance with the obligations set out in this DPA shall be documented through reports containing relevant information, including copies of the then most recent third-party audits or certifications set forth in the Trust Centre.

To the extent that the report is not sufficient to demonstrate compliance with the obligations set out in this DPA, and where Data Protection Law grants the controller a right to conduct audits, the controller may request an audit, including on-site audits, in accordance with the terms of the DPA Section 8, and processor shall permit and contribute to such on-site audits of the processing activities covered by this DPA.

Requests for on-site audits under Section 8 of this DPA should be directed to privacy@boost.ai.

All audits will be limited to the processing of controller´s personal data and storage and processing facilities operated by boost.ai. The on-site audit shall be conducted by controller or its third party auditor:

- acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by the controller;
- up to one time per 12 months, or more frequently where the controller has received a notification from the processor of a personal data breach, or where Data Protection Laws or the controller's competent supervisory authority require that audits be conducted more frequently;
- with at least thirty (30) days advance written notice setting out the scope;
- during boost.ai´s normal business hours, for a reasonable duration and shall not unreasonably interfere with boost.ai´s day-to-day operations;

Before any on-site audit commences, the controller and boost.ai shall mutually agree upon the scope, the timing and duration of the audit.

Each Party shall bear its own reasonable costs relating to an audit. Where an audit conducted at the controller's request requires extraordinary effort or resources on the part of the processor, beyond what is reasonably required to verify compliance, the controller shall bear the reasonable additional costs thereby incurred by the processor.

Where the controller wishes to use a third party auditor to conduct an audit, prior to conducting the audit the third party auditor will be required to enter into a non-disclosure agreement with boost.ai. All costs relating to the controller's use of a third-party auditor will be covered by the controller.

The controller must promptly provide boost.ai with all information regarding any non-compliance discovered during the course of an on-site audit.

B. Sub-processor notifications

To receive notifications regarding sub-processor updates according to the DPA section 9.2, the controller shall subscribe to updates from the boost.ai Trust Center, where the sub-processor list referred in section 9.1 is published. The controller is responsible for ensuring that it discloses the correct contact information and keeps the contact information complete, accurate and up to date. The controller can subscribe to Trust Center updates with multiple email addresses.

C. Transfer of European Personal Data

C.1 boost.ai as data exporter and boost.ai's sub-processor as data importer

Transfer of personal data where boost.ai is the data exporter and our sub-processor is the data importer may occur if the controller appoints sub-processors located in third countries, as specified in the agreed list referenced in the DPA section 9.1.

Boost.ai has currently identified two cases where such a transfer may occur:

1. The customer receives support from the boost.ai subsidiary BT AI UK Ltd
2. The customer chooses the US as a processing location for a sub-processor

For case nr. 1, the following transfer mechanism is the default:

The sub-processor is a company established in the United Kingdom and that the sub-processor will access personal data stored on the location described in Annex II from the United Kingdom. Such access constitutes a transfer of personal data to a third country within the meaning of Chapter V of the GDPR.

For as long as, and to the extent that, the European Commission's adequacy decision for the United Kingdom under Article 45 of Regulation (EU) 2016/679 (currently Commission Implementing Decision (EU) 2021/1772, as amended, replaced, or succeeded from time to time) remains in force and covers the transfer in question, such transfer may take place on the basis of that adequacy decision without the need for any further transfer mechanism or safeguard under Chapter V of Regulation (EU) 2016/679. Where the European Commission adopts a new or successor adequacy decision covering the United Kingdom in place of the decision referred to above, such new or successor decision shall be deemed to be the applicable adequacy decision for the purposes of this clause 12, and the transfer shall continue to take place on that basis without interruption.

Where personal data of Swiss data subjects, or personal data otherwise subject to the Swiss Federal Act on Data Protection ("nFADP"), is transferred by the processor or their sub-processors to a third country, such transfer shall, for as long as and to the extent that the United Kingdom is listed as

ensuring an adequate level of data protection under Annex 1 of the Swiss Data Protection Ordinance (DSV), take place on the basis of that adequacy listing, without the need for any further transfer mechanism under the nFADP.

For case nr. 2, the following transfer mechanism is the default:

For as long as, and to the extent that, the sub-processor is certified under the European Commission's adequacy decision for the United States under Article 45 of Regulation (EU) 2016/679 (currently Commission Implementing Decision (EU) 2023/1795 (the EU-U.S. Data Privacy Framework, as amended, replaced, or succeeded from time to time), the remains in force and covers the transfer in question, such transfer may take place on the basis of that adequacy decision without the need for any further transfer mechanism or safeguard under Chapter V of Regulation (EU) 2016/679. Where the European Commission adopts a new or successor adequacy decision covering the United States in place of the decision referred to above, such new or successor decision shall be deemed to be the applicable adequacy decision, and the transfer shall continue to take place on that basis without interruption.

Fallback transfer mechanism for cases 1 and 2:

If, and for so long as, no adequacy decision is in force and covers the transfer in question, whether because the decision is suspended, repealed, amended so as no longer to cover the transfer, invalidated, or otherwise ceases to apply or to constitute a valid transfer mechanism under Applicable Data Protection Law, and no new or successor adequacy decision covering the transfer has been adopted, the controller hereby instructs and authorises boost.ai to enter into, and to ensure that the relevant sub-processor enters into, Module Three (processor-to-processor) of the Standard Contractual Clauses ("SCCs") adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, as the transfer mechanism between boost.ai (as data exporter) and the relevant sub-processor (as data importer). SCCs as transfer mechanism shall take effect automatically upon the fallback event described above, without the need for further instruction, signature, or agreement from the controller.

Where personal data of Swiss data subjects, or personal data otherwise subject to the Swiss Federal Act on Data Protection ("nFADP"), is transferred, the controller hereby instructs and authorises boost.ai to ensure that the SCCs referred to above, as entered into between boost.ai and the relevant sub-processor, are supplemented by the amendments necessary to render them valid as a transfer mechanism under the nFADP (a "Swiss Addendum").

Where personal data subject to the UK GDPR and the UK Data Protection Act 2018 is transferred, the controller hereby instructs and authorises boost.ai to ensure that the SCCs referred to above, as entered into between boost.ai and the relevant sub-processor, are supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (the "UK Addendum"), which will render the SCCs valid as a transfer mechanism under UK data protection law.

C.2 Controller as data exporter and boost.ai as data importer

Boost.ai has identified that for customers established in the U.S., who contract with Boost.ai, Inc., the processing of European personal data will constitute a Third-Country Transfer where boost.ai is the data importer and the customer is the data exporter.

To ensure an adequate level of protection for the transferred personal data, the Parties agree to enter into and incorporate the Standard Contractual Clauses ("SCCs") adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 which are incorporated by reference and form an integral part of this DPA.

Module Two (transfer controller to processor) of the SCCs shall apply. In addition, the following shall apply: the optional Clause 7 (docking clause) is not included; Clause 9(a) is included as Option 2 (General Written Authorisation), pursuant to which Boost.ai, Inc. (as data importer) has the controller's general authorisation for the engagement of sub-processors from the agreed list referred in section 9.1 of the DPA, and shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 (thirty) days in advance, using the mechanism described in the DPA Annex I section B, thereby giving the controller sufficient time to object to such changes prior to the engagement of the sub-processor(s), and Boost.ai, Inc. shall provide the controller with the information necessary to enable the controller to exercise its right to object; the duration of transfer is the same as the duration of processing as described in Annex II to this DPA. The optional paragraph in Clause 11(a) (independent dispute resolution body) is not included. Unless otherwise agreed in writing, Clause 17 is included as Option 1, and governing law shall be the law of Norway, and the Norwegian Data Protection Authority shall be the competent supervisory authority. The information required under Annex I.A (List of Parties) of the SCCs is set out in the Agreement and/or the applicable Order Form; the information required under Annex I.B (Description of Transfer) of the SCCs is deemed to be set out in Annex II to this DPA (Description of the Processing); the information required under Annex I.C (Competent Supervisory Authority) of the SCCs is as set out in this Clause C.2; and the information required under Annex II (Technical and Organisational Measures) of the SCCs is deemed to be set out in the security measures referenced in section 6 of this DPA.

Where personal data of United Kingdom data subjects, or personal data otherwise subject to the UK GDPR and the Data Protection Act 2018, is transferred, the SCCs shall apply as the transfer mechanism, supplemented and modified by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (the "UK Addendum"), the terms of which are hereby incorporated by reference and deemed entered into between the controller and boost.ai Inc. upon execution of this DPA, The information required under the UK Addendum, insofar as it corresponds to Annex I.A (List of Parties) of the SCCs, is set out in the Agreement and/or the applicable Order Form; insofar as it corresponds to Annex I.B (Description of Transfer) of the SCCs, is deemed to be set out in Annex II to this DPA (Description of the Processing); insofar as it corresponds to Annex I.C (Competent

Supervisory Authority) of the SCCs, is as set out in this Clause C.2; and insofar as it corresponds to Annex II (Technical and Organisational Measures) of the SCCs, is deemed to be set out in the security measures referenced in section 6 of this DPA. The controller, as the exporting party, remains responsible for carrying out any data protection test (transfer risk assessment) required under UK data protection law prior to the transfer.

Where personal data of Swiss data subjects, or personal data otherwise subject to the Swiss Federal Act on Data Protection ("nFADP"), is transferred, the SCCs shall apply, subject to the amendments necessary to render them valid as a transfer mechanism under the nFADP (a "Swiss Addendum"), including the following: (i) references to the "GDPR" shall be understood to include the nFADP where the context so requires; (ii) references to the "competent supervisory authority" shall include the Swiss Federal Data Protection and Information Commissioner (FDPIC) with respect to transfers subject to the nFADP; (iii) references to "data subjects" shall include data subjects in Switzerland; and (iv) the term "Member State" shall not be interpreted to exclude the rights of data subjects in Switzerland from enforcing their rights in their place of habitual residence. The information required under Annex I.A (List of Parties) of the SCCs is set out in the Agreement and/or the applicable Order Form; the information required under Annex I.B (Description of Transfer) of the SCCs is deemed to be set out in Annex II to this DPA (Description of the Processing); the information required under Annex I.C (Competent Supervisory Authority) of the SCCs is, for transfers subject to the nFADP, the FDPIC as set out above; and the information required under Annex II (Technical and Organisational Measures) of the SCCs is deemed to be set out in the security measures referenced in section 6 of this DPA. The controller, as the exporting party, remains responsible for carrying out any transfer impact assessment required under the nFADP prior to the transfer. Unless otherwise agreed by the Parties, Swiss law shall govern the SCCs to the extent they are used to transfer personal data protected by the nFADP, and the FDPIC shall be the competent supervisory authority for such transfers.

D. Personal data breach notification

Notification of personal data breach according to the DPA section 12 shall be sent using the contact details disclosed by the controller in the Admin Panel. The controller is responsible for ensuring that it discloses the correct contact information and keeps the contact information in the Admin Panel complete, accurate and up to date.

E. Notification of changes to this Annex I

Notifications of changes to this Annex I according to the DPA section 14 shall be sent using the contact details disclosed by the controller in the Admin Panel. The controller is responsible for ensuring that it discloses the correct contact information and keeps the contact information in the Admin Panel complete, accurate and up to date.

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

The categories of data subjects are End Users, and Admin Panel users which typically includes Customers employees, consultants or other representatives.

Categories of personal data processed

The type of data is any type of data submitted by, sent to, or received by controller or End Users through the Solution, including End User voices if voice services are used, as well as information about the users of the admin panel.

Sensitive data

No sensitive data is required in order to provide the Services. However, due to the nature of the services and the possibility of processing open text, sensitive personal data may be processed if provided by the End User. The additional safeguards are made available by the processor and must be adjusted accordingly by the controller or its representative directly into the Admin Panel.

Nature of the processing

The nature of the data processing is computing, storage and other processing necessary to provide, maintain and improve the services provided by the processor to the controller under the Agreement. Also, disclosure in accordance with the Agreement and/or as necessary to comply with applicable laws and regulations.

Purpose(s) for which the personal data is processed on behalf of the controller

The purpose of data processing under this DPA is the provision and improvement of the Services offered and made available to controller as a software as a service (SaaS) as established by the Agreement, or as subsequently instructed by the controller

The processor is hereby given a permission to anonymize Personal Data from the assignment and reuse the anonymized data, provided that the data is no longer information relating to an identified or identifiable natural person. The anonymized data can be used for, i.a., the purpose of analyzing, developing and improving artificial intelligence models, algorithms, and related technologies. Strict information security measures will be used in connection with the processing.

Controller acknowledges and agrees that when using the voice services, boost.ai's sub-processor, Twilio, may aggregate and anonymize data and use that aggregated and anonymized data to develop and improve new products and services and improve the performance, functionality, safety,

and security of their services. For the avoidance of doubt, Twilio does not have access to Customer content transmitted through the services in connection with the voice offering.

Duration of the processing

The processor will be processing data under this DPA for as long as the processor processes data on behalf of the controller in accordance with the Agreement, and in accordance with the controllers adjustments of the retention settings in the Admin Panel.