CHASSI

DATA PROCESSING ADDENDUM

(Effective Date: Jan. 09, 2025)

This Data Processing Addendum, including its Schedules, (“DPA”) amends and supplements the Agreement between Chassi and Customer (together, the “Agreement”) to which it is attached, to reflect the parties’ agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Chassi processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Chassi may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

“Chassi” means SaaS Industries, Inc. (d.b.a. “Chassi”), a company incorporated in Delaware, USA.

“Agreement” means any services agreement including, but not limited to, Chassi’s Order Form and Services Agreement, or other services agreement between Chassi and Customer under which the Service is provided by Chassi to Customer.

“Authorized Affiliate” means any of Customer's Affiliate(s) (as defined in the Agreement) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Canada, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Chassi but has not signed its own Order Form with Chassi and is not a "Customer" as defined under the Agreement.

“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.

“Chassi” means SaaS Industries, Inc. (d.b.a. “Chassi”), a company incorporated in Delaware, USA.

“Chassi Platform” means Chassi’s proprietary cloud-based web application and analysis engine.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Customer” means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates).

“Customer Data” means what is defined in the Agreement as “Customer Data”, provided that such data is electronic data and information submitted by or for Customer to the Services.

“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, the United Kingdom and the United States and its states.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“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 (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), where for each (i) or (ii), such data is Customer Data.

“Processing” 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, 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.

“Public Authority” means a government agency or law enforcement authority, including judicial authorities.

“Security Measures” means the security measures applicable to the specific Services purchased by Customer, as updated from time to time, including at minimum the measures set forth in Annex II.

“Services” means access to Chassi’s cloud-based, AI-powered process intelligence tools or related services performed pursuant to the Agreement.

“Standard Contractual Clauses” means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

“Sub-processor” means any Processor engaged by Chassi. As of the Effective Date, Sub-processors are listed in Schedule 3.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Chassi is the Processor and that Chassi will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2 Customer’s Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Chassi as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the Data Protection Laws.

2.3 Chassi’s Processing of Personal Data. Chassi shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Chassi is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex I (Details of the Processing) to this DPA.

2.5 Customer Instructions. Chassi shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Chassi is unable to follow Customer’s instructions for the Processing of Personal Data.

3. RIGHTS OF DATA SUBJECTS

Chassi shall, to the extent legally permitted, promptly notify Customer if Chassi receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, Chassi shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Chassi shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Chassi is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Chassi's provision of such assistance.

4. CHASSI PERSONNEL

4.1 Confidentiality. Chassi shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Chassi shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Chassi shall take commercially reasonable steps to ensure the reliability of any Chassi personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Chassi shall ensure that Chassi's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Data Protection Officer. Chassi has appointed Justin Dooley as data protection officer (DPO). Justin may be reached at privacy@chassi.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Chassi's Affiliates may be retained as Sub-processors; and (b) Chassi and Chassi's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Chassi or a Chassi Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Chassi's current list of Sub-processors for the Services is set forth at https://chassi.com/legal-dpa/subprocessors. Such Sub-processor list includes the identities of those Sub-processors and their country of location. Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains

to their Personal Data. Customer must enroll at the aforementioned URL to receive email notifications concerning the addition of new Sub-processors.

5.3 Objection Right for New Sub-processors. Customer may object to Chassi's use of a new Sub-processor by notifying Chassi promptly in writing at privacy@chassi.com within fifteen (15) days after receipt of Chassi's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Chassi will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Chassi is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement(s) with respect only to those Services which cannot be provided by Chassi without the use of the objected-to new Sub-processor by providing written notice to Chassi. Chassi will refund Customer any prepaid fees covering the remainder of the term of such Agreement(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4 Liability. Chassi shall be liable for the acts and omissions of its Sub-processors to the same extent Chassi would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Chassi shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security Measures. Chassi regularly monitors compliance with these measures. Chassi will not materially decrease the overall security of the Services during a subscription term.

6.2 Audit. Chassi shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA, including those obligations required by applicable Data Protection Laws, as set forth in this section 6.2.

6.2.1 Third-Party Certifications and Audits. Chassi is certified ISO 27001:2022 compliant and audited annually for SOC 2 Type 2 with Security and Privacy Trust Services Criteria and agrees to maintain an information security program for the Services that complies with the standards defined within each of our audits and certifications. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Chassi shall make available to Customer, that is not a competitor of Chassi (or Customer's independent, third-party auditor that is not a competitor of Chassi), a copy of Chassi's most recent third-party audits or certifications, as applicable. Such third-party audits or

certifications may also be shared with Customer's competent supervisory authority on its request. Upon request, Chassi shall also provide a requesting Customer with a report and/or confirmation of Chassi's audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Chassi, to the extent such reports or evidence may be shared with Customer ("Third-party Sub-processor Audit Reports"). Customer acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Chassi may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.2.2 Data Processing Audit. Customer may contact Chassi to request an audit of Chassi's Processing activities covered by this DPA ("Data Processing Audit"). The Data Processing Audit may be conducted by Customer either itself or through a Third-Party Auditor (as defined below in section 6.2.4) selected by Customer when:

(i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;

(ii) Customer has received a notice from Chassi of a Customer Data Incident; or

(iii) such an audit is required by Data Protection Laws or by Customer's competent supervisory authority. Any Data Processing Audits will be limited to Customer Data Processing activities by Chassi and relevant control activities to conduct said Processing as referenced in this DPA. Customer acknowledges that Chassi operates a multi-tenant cloud environment. Accordingly, Chassi shall have the right to reasonably adapt the scope of any Data Processing Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Chassi customers' information.

6.2.3 Reasonable Exercise of Rights. A Data Processing Audit shall be conducted by Customer or its Third-Party Auditor:

(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Customer;

(ii) up to one time per year with at least thirty (30) days written notice. If an emergency justifies a shorter notice period, Chassi will use good faith efforts to accommodate the Data Processing Audit request; and

(iii) during Chassi's normal business hours, under reasonable duration and shall not unreasonably interfere with Chassi's day-to-day operations. Before any Data Processing Audit commences, Customer and Chassi shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which

Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Chassi.

6.2.4 Third-Party Auditor. A Third Party Auditor means a third-party independent contractor that is not a competitor of Chassi. A Data Processing Audit can be conducted through a Third Party Auditor if: (i) prior to the Data Processing Audit, the Third Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Chassi's proprietary information; and (ii) the costs of the Third Party Auditor are at Customer's expense.

6.2.5 Findings. Customer must promptly provide Chassi with information regarding any non-compliance discovered during the course of a Data Processing Audit.

6.3 Data Protection Impact Assessment. Upon Customer's request, Chassi shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Chassi.

7. CUSTOMER DATA BREACH MANAGEMENT AND NOTIFICATION

Chassi maintains security incident management policies and procedures specified in the Security Measures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Chassi or its Sub-processors of which Chassi becomes aware (a "Customer Data Breach"). Chassi shall make reasonable efforts to identify the cause of such Customer Data Breach and take those steps as Chassi deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Chassi's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. GOVERNMENT ACCESS REQUESTS

8.1 Chassi Requirements. In its role as a Processor, Chassi shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Chassi receives a legally binding request to access Personal Data from a Public Authority, Chassi shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent Chassi is prohibited by law from providing such notification, Chassi shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Chassi to communicate

as much information as possible, as soon as possible. Further, Chassi shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Chassi shall pursue possibilities of appeal. When challenging a request, Chassi shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Chassi agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Chassi shall promptly notify Customer if Chassi becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Chassi in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Chassi to pursue action or inaction that could result in civil or criminal penalty for Chassi such as contempt of court. Chassi certifies that Chassi (1) has not purposefully created back doors or similar programming for the purpose of allowing access to the Services and/or Personal Data by any Public Authority; (2) has not purposefully created or changed its business processes in a manner that facilitates access to the Services and/or Personal Data by any Public Authority; and (3) at the Effective Date is not currently aware of any national law or government policy requiring Chassi to create or maintain back doors, or to facilitate access to the Services and/or Personal Data, to keep in its possession any encryption keys or to hand-over the encryption key to any third party.

8.2 Sub-processors requirements. Chassi shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

9. RETURN AND DELETION OF CUSTOMER DATA

Chassi shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement. Until Customer Data is deleted or returned, Chassi shall continue to comply with this DPA and its Schedules.

10. AUTHORIZED AFFILIATES

10.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Chassi and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Chassi under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Chassi, it shall to the extent required under applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1 Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Chassi directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in Section 10.3.2, below).

10.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Chassi and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Chassi, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Chassi's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

12. EUROPEAN SPECIFIC PROVISIONS

12.1 Definitions. For the purposes of this Section 12 these terms shall be defined as follows:

"EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

"EU P-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

12.2 GDPR. Chassi will Process Personal Data in accordance with the GDPR requirements directly applicable to Chassi's provision of its Services.

12.3 Standard Contractual Clauses for data transfers. Chassi applies the Standard Contractual Clauses to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws.

12.3.1 The EU C-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Chassi is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU C-to-P Transfer Clauses.

12.3.2 The EU P-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Chassi is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of the EU P-to-P Transfer Clauses.

12.4 The following additional terms apply with respect to the Standard Contractual Clauses:

12.4.1 Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 12.5 apply to (i) Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, and (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Section 12, Customer is the “data exporter” and Chassi is the “data importer”. If and to the extent an Authorized Affiliate relies on the Standard Contractual Clauses for the transfer of Personal Data, any references to ‘Customer’ in this DPA, include such Authorized Affiliate.

12.4.2 Reference to the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 1.

12.4.3 Docking clause. The option under clause 7 of the Standard Contractual Clauses shall not apply.

12.4.4 Instructions. This DPA and the Agreement are Customer’s complete and final documented instructions at the time of signature of the Agreement to Chassi for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1(a) of the Standard Contractual Clauses, the instructions by Customer to Process Personal Data are set out in section

2.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

12.4.5 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Chassi to Customer only upon Customer's written request.

12.4.6 Security of Processing. For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in the Security Measures meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Chassi provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Breach Management and Notification) of this DPA.

12.4.7 General Authorisation for Use of Sub-Processors. Option 2 under Clause 9 shall apply. For purposes of clause 9(a), Chassi has Customer's general authorisation to engage Sub-processors in accordance with section 5 of this DPA. Chassi shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA. Chassi shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA. Chassi shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

12.4.8 Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Chassi may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Chassi shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

12.4.9 Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by Chassi to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Chassi beforehand; and, that such copies will be provided by Chassi, in a manner to be determined in its discretion, only upon request by Customer.

12.4.10 Audits and Certifications. The parties agree that the audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with section 6.2 of this DPA.

12.4.11 Complaints - Redress. For the purposes of Clause 11, and subject to section 3 of this DPA, Chassi shall inform data subjects on its website of a contact point authorised to handle complaints. Chassi shall inform Customer if it receives a

complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Chassi shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

12.4.12 Liability. Chassi's liability under clause 12(b) shall be limited to any damage caused by its Processing where Chassi has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

12.4.13 Supervision. Clause 13 shall apply as follows:

12.4.13.1 Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

12.4.13.2 Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

12.4.13.3 Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as competent supervisory authority.

12.4.13.4 Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

12.4.13.5 Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

12.4.14 Notification of Government Access Requests. For the purposes of clause 15(1)(a), Chassi shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

12.4.15 Governing Law. The governing law for the purposes of Clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the

Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of France; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

12.4.16 Choice of forum and jurisdiction. The courts under Clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) France; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

12.4.17 Appendix. The Appendix shall be completed as follows:

- The contents of section A (List of Parties) of Schedule 1 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections B (Description of the Processing/Transfer) of Schedule 1 shall form Annex I.B to the Standard Contractual Clauses
- The contents of Section 12.5.13 (Supervision) above shall form Annex I.C to the Standard Contractual Clauses
- The contents of Schedule 3 (List of Sub-processors) to this Exhibit shall form Annex II to the Standard Contractual Clauses.

12.4.18 Data Exports from the United Kingdom under the Standard Contractual Clauses. For data transfers governed by UK Data Protection Laws and Regulations, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 1 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

12.4.19 Data Exports from Switzerland under the Standard Contractual Clauses. For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

12.4.20 Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.5 Additional Terms for the EU P-to-P Clauses. For the purposes of the EU P-to-P Transfer Clauses (only), the Parties agree the following.

12.5.1 Instructions and notifications. For the purposes of clause 8.1(a), Customer hereby informs Chassi that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Chassi for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Chassi to the relevant Controller where appropriate.

12.5.2 Security of Processing. For the purposes of clause 8.6(c) and (d), Chassi shall provide notification of a personal data breach concerning Personal Data Processed by Chassi to Customer.

12.5.3 Documentation and Compliance. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Chassi by Customer. If Chassi receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

12.5.4 Data Subject Rights. For the purposes of Clause 10 and subject to section 3 of this DPA, Chassi shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

12.6 Impact of Local Laws. As of the Effective Date, Chassi has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorising access by a Public Authority, prevent Chassi from fulfilling its obligations under this DPA. If Chassi reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Chassi shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Chassi is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot

be provided by Chassi in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services

13. UNITED STATES SPECIFIC PROVISIONS

13.1 Customer Instructions. The parties acknowledge that Customer discloses Personal Data to Chassi for the limited and specified purposes set forth in the Agreement and DPA, and as instructed by Customer.

13.2 Customer Rights. Customer shall have the right to take the reasonable and appropriate steps set forth in the Agreement designed to stop and remediate unauthorized use of Personal Data.

13.3 Chassi's Processing of Personal Data. Chassi will not retain, use, disclose, sell, or share the Personal Data other than providing the Services specified by Customer's documented instructions. Chassi will not combine Personal Data with information received from, or on behalf of other entities, except to perform the purpose of providing the Services specified by Customer's documented instructions. Chassi shall Process Personal Data in accordance with Data Protection Laws applicable to Chassi's provision of the Services to its customers generally (i.e., without regard for Customer's particular use of the Services), when the Services are used according to this DPA, the Agreement, the Documentation, and the applicable Order Form. Chassi shall inform Customer if Chassi determines it is unable to meet its obligations under the CCPA.

14. CANADA SPECIFIC PROVISIONS

To the extent that the Personal Information Protection and Electronic Documents Act (PIPEDA) applies, Chassi agrees to collect, use, and disclose personal information only with valid consent and for the limited purposes identified, ensuring its accuracy and security. Chassi further commits to, in coordination with the Customer, facilitating data subject rights, promptly addressing inquiries or complaints, and cooperating to ensure compliance with PIPEDA principles.

15. PARTIES TO THIS DPA

Where the Standard Contractual Clauses are applicable, SaaS Industries, Inc. (d.b.a. "Chassi") is the signatory to the Standard Contractual Clauses. Where the Chassi entity that is a party to this DPA is not SaaS Industries, Inc, that Chassi entity is carrying out the obligations of the data importer on behalf of SaaS Industries, Inc.

List of Schedules

Schedule 1: Description of the Processing/Transfer

Schedule 2: Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of The Data

Schedule 3: List of Sub-Processors

SCHEDULE 1 – DESCRIPTION OF PROCESSING/TRANSFER

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Entity Name: _____

Address: _____

Contact Person's Name: _____

Contact Person's Email: _____

Description of Relevant Data Export Activities: _____

Signature: _____

Date: _____

Role (Controller/Processor): _____

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Entity Name: SaaS Industries, Inc. (d.b.a. "Chassi")

Address: 15333 N Pima Rd Scottsdale AZ 85260

Contact Person's Name: Justin Dooley

Contact Person Email: privacy@chassi.com

Description of Relevant Data Import Activities:

- Chassi is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Signature: _____

Date: _____

Role (Controller/Processor): Processor

DESCRIPTION OF PROCESSING/TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer Users authorized by Customer to use the Services, which may include data exporter's customer's representatives and end users.

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Name
- Address
- Email address
- Phone number
- Company name
- Title
- _____
- _____

In addition, Data Exporter may define additional fields and has control over the type of information such fields may contain. However, Data Exporter should not define or submit any special categories of data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having

followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis or alternate frequency as defined by the Agreement with Customer.

Nature of the processing

- Chassi will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Purpose(s) of the data transfer and further processing

- The objective of Processing of Personal Data by data importer is the performance of business process optimization services pursuant to the Agreement and Schedules of Work.

The duration of the processing

- Subject to Section 8 of the DPA, Chassi will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Personal Data will be retained for the length of the Agreement, or in accordance with applicable Data Privacy Laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors shall Process Personal Data for purposes of assisting Chassi in providing the Services to Customer under the Agreement and shall continue to process Personal Data for the length of the applicable agreement governing provision of the Services or as otherwise required under applicable Data Privacy Laws.

Identify the competent supervisory authority/ies in accordance with clause 13:

- The supervisory authority specified in section 12.5.13 of the DPA shall act as the competent supervisory authority.

SCHEDULE 2 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Security Measures Chassi implements to protect Customer Personal Data are set out in Chassi System's Security Policy. This policy is subject to change to industry standards and best practices are updated. The latest version of this policy can be found in the Chassi customer service portal. A current version of the Security Policy as of the Effective Date of this DPA is set forth below:

CHASSI SECURITY POLICY

This Chassi Security Policy (the "Security Policy") outlines the technical and procedural safeguards that Chassi undertakes to protect Customer Data from unauthorized access or disclosure. Chassi maintains these Security Measures in a manner consistent with SOC 2 and ISO 27001:2022. This Security Policy is referenced in and made a part of your customer agreement with Chassi (the "Agreement"). In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern. Capitalized terms used but not defined in this Security Policy have the meanings set forth in the Agreement or in the Documentation.

1. CUSTOMER DATA ACCESS AND MANAGEMENT

1.1. Access to Chassi production systems and production data, including Personal Data, are restricted according to the principle of least privilege unless Customer provides access to its Chassi account to such Chassi Personnel. “Chassi Personnel” means Chassi employees and individual subcontractors engaged in the Processing of Personal Data. Chassi uses Customer Data only as necessary to provide the Chassi Service to Customer, as provided in the Agreement.

1.2. Customer Data stored on the Chassi Platform is managed via Amazon Web Services’ ISO 27001 certified data centers and hosted in the region US-East-1 (N. Virginia).

1.3. Chassi shall create and maintain flow diagram(s) indicating how Customer Data flows through the Chassi Service. Chassi shall provide such flow diagram(s) upon Customer’s reasonable request.

2. ENCRYPTION AND LOGICAL SEPARATION OF CUSTOMER DATA

2.1. The Chassi Service in the production storage environment always encrypts Customer Data while at rest with Amazon’s EBS encryption functionality.

2.2. The Chassi Service encrypts Customer Data in transit using TLS when communicating across untrusted networks such as the Public Internet.

2.3. All database servers are isolated inside virtual private networks, and accessible only by key personnel via multi-factor authentication.

2.4. The Chassi Service assigns a unique Customer ID for each client on the Chassi Platform. All end customer data is stored with this Customer ID as a direct or chained foreign key in our database. This Chassi Platform's application's data model is designed with multi-tenancy as a requirement.

2.5. Encryption keys and key encrypting keys are logically separated from Customer Data. Chassi safeguards top level encryption keys by tightly managing key access and utilizing regular rotation mechanisms as described by our policies and procedures.

3. CHASSI SERVICE INFRASTRUCTURE ACCESS MANAGEMENT

3.1. Access to the systems and infrastructure that support the Chassi Platform is restricted to Chassi Personnel who require such access as part of their job responsibilities.

3.2. Unique User IDs are assigned to Chassi Personnel requiring access to the Chassi servers that support the Chassi Platform.

3.3. Access privileges of separated Chassi Personnel are disabled in a timely manner as described by our policies and procedures. Additionally, access privileges of persons transferring to jobs requiring reduced privileges are adjusted accordingly.

3.4. Two-factor authentication is supported and is mandatory for all internal administrator functions of the application.

3.5. User access to the systems and infrastructure that support the Chassi Service is reviewed quarterly.

3.6. Access attempts to the systems and infrastructure that support the Chassi Service are logged and monitored. All login pages have brute-force logging and protection.

3.7. AWS Security Groups have deny-all default policies and only enable business required network protocols for egress and ingress network traffic.

4. RISK MANAGEMENT

4.1. Chassi conducts risk assessments of various kinds throughout the year, including self- and third-party assessments and tests, automated scans, and manual reviews.

4.2. Results of assessments, including formal reports as relevant, are reported to the information security officer (ISO). A Security Steering Committee meets at least annually to review reports, identify control deficiencies and material changes in the threat environment, and make recommendations for new or improved controls and threat mitigation strategies to senior management.

4.3. Changes to controls and threat mitigation strategies are evaluated and prioritized for implementation on a risk-adjusted basis. All code changes to applications require

testing via an enforced testing process, including high-level server penetration tests across various parts of our platform, as well as security-focused code reviews.

4.4. Threats are monitored through various means, including threat intelligence services, vendor notifications, and trusted public sources.

5. VULNERABILITY SCANNING AND PENETRATION TESTING

5.1. Static and dynamic code scans are executed looking for OWASP top 10 vulnerabilities prior to new code being released into our environments.

5.2. Vulnerability scans are automatically and regularly performed on systems required to operate and manage the Chassi Platform. The vulnerability database is updated regularly.

5.3. Potential impact of vulnerabilities that trigger alerts are evaluated by technical staff.

5.4. Vulnerabilities that trigger alerts and have published exploits are reported to the chief technology officer (CTO), which determines and supervises appropriate remediation action.

5.5. Security management monitors or subscribes to trusted sources of vulnerability reports and threat intelligence.

5.6. Penetration tests by an independent third-party expert are conducted at least annually.

6. CHASSI SERVICE LOCATION

6.1. Customer Data is stored in Amazon Web Services' certified data centers and hosted in the region US-East-1 (N. Virginia).

7. SYSTEM EVENT LOGGING

7.1. Monitoring tools and services are used to monitor systems including network, server events, and AWS security events, availability events, and resource utilization.

7.2. Chassi infrastructure Security Event Logs are collected in a central system and protected from tampering. Logs are stored for 12 months.

7.3. All security logs are written to a central cloud service and are immutable.

8. SYSTEM ADMINISTRATION AND PATCH MANAGEMENT

8.1. Chassi shall create, implement and maintain system administration procedures for systems that access Customer Data that meet or exceed industry standards, including without limitation, system hardening, system and device patching (operating system and applications) and proper installation of threat detection software as well as daily signature updates of the same.

8.2. Chassi reviews all open “high” or “critical” infrastructure vulnerabilities on a quarterly basis and creates remediation plans to address those vulnerabilities or risk accept them based on a defined risk management methodology.

9. CHASSI SECURITY TRAINING AND CHASSI PERSONNEL

9.1. Chassi maintains a security awareness program for Chassi Personnel, which provides initial education, ongoing awareness and individual Chassi Personnel acknowledgment of intent to comply with Chassi System's corporate security and privacy policies. New hires sign a confidentiality agreement, and digitally sign various policies that cover key aspects of the Security Policy.

9.2. All Chassi Personnel acknowledge they are responsible for reporting actual or suspected security incidents or concerns, thefts, breaches, losses, and unauthorized disclosures of or access to Customer Data.

9.3. All Chassi Personnel are required to satisfactorily complete annual security training.

9.4. Chassi performs criminal background screening as part of the Chassi hiring process, to the extent legally permissible.

9.5. Chassi will ensure that its subcontractors, vendors, and other third parties that have direct access to the Customer Data in connection with the Services adhere to the same security standards in place for Chassi employees.

10. PHYSICAL SECURITY

10.1. The Chassi Platform is hosted on AWS. All physical security controls are managed by AWS. Chassi reviews the SOC 2 Type 2 report annually to ensure appropriate physical security controls:

10.1.1. Visitor management including tracking and monitoring physical access.

10.1.2. Physical access points to server locations are managed by electronic access control devices.

10.1.3. Monitor and alarm response procedures.

10.1.4. Use of CCTV cameras at facilities.

10.1.5. Video capturing devices in data centers with 90 days of image retention.

11. NOTIFICATION OF CUSTOMER DATA BREACH

11.1. Chassi will notify Customer in writing within forty-eight (48) hours of a confirmed Customer Data Breach.

11.2. Such notification will describe the Customer Data Breach and the status of Chassi investigation.

11.3. Chassi will take appropriate actions to contain, investigate, and mitigate the Customer Data Breach.

12. BUSINESS CONTINUITY AND RESILIENCE

12.1. Chassi maintains Business Continuity and Resilience plans for the Chassi Platform. These plans are tested annually.

12.2. Chassi conducts an annual business impact analysis (“BIA”) on all systems supporting Services to identify their criticality and RPO / RTO.

13. CHASSI SECURITY, CERTIFICATIONS, AND THIRD-PARTY ATTESTATIONS

13.1. Chassi hires accredited third parties to perform audits and to attest to various compliance frameworks and certifications annually, including:

13.1.1. SOC 2 Type II

13.1.2. ISO 27001:2022

14. CUSTOMER RESPONSIBILITIES

14.1. Customer is responsible for managing its own user accounts and roles within the Chassi Platform and for protecting its own account and user credentials. Customer will comply with the terms of its Agreement with Chassi as well as all applicable laws.

14.2. Customer will promptly notify Chassi if a user credential has been compromised or if Customer suspects possible suspicious activities that could negatively impact security of the Chassi Platform or Customer's account. Customer may not perform any security penetration tests or security assessment activities without the express advance written consent of Chassi.

14.3. Customer is responsible for adhering to the defined SOC 2 user entity controls.

14.4. Customer is responsible for maintaining the relationship and ensuring that all necessary agreements (i.e. Data Processing Agreements) are in place with other Processors that the Customers engage with and transmit Personal Data to, through their use of Chassi Services.

Schedule 3 - List of Sub-processors

Chassi uses its Affiliates and a range of third-party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors as of the Effective Date of this DPA are set out below. These Sub-processors are listed below and regularly updated at https://chassi.com/legal-dpa/subprocessors/.

Service Provider Name	Business Purpose	Information Collected by the Service Provider	Data Location	Public DPA Link
Amazon Web Services	Cloud Service Provider	Contact information; technical identifiers	United States	AWS DPA (Public)
Google Workspace	Business productivity	Contact information; technical identifiers	United States	Google Workspace DPA (Public)
HotJar	Platform Usage Analytics	Technical identifiers, screen recording	United States	HotJar Ltd. DPA (Public)
HubSpot	Marketing, Customer Relations Management and Customer Service	Contact information; technical identifiers	United States	HubSpot DPA (Public)
Revolear	Contract management	Billing contact, signatures	United States	Revolear DPA (Public)
Slack	Collaboration and Communications	Contact information; technical identifiers	United States	Slack Technologies DPA (Public)
Squarespace	Domain Hosting	Technical identifiers	United States	Squarespace DPA (Public)
WordPress	Website Hosting	Contact information; technical identifiers	United States	WordPress DPA (Public)
Zoom	Collaboration and Communications	Contact information; voice and/or screen recording	United States	Zoom DPA (Public)