Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the PaaS Services Agreement (the "Agreement") between Customer and Tecton, Inc., a Delaware corporation (the "Company") (together as the "Parties").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA.

1. Definitions.

"Customer Data" means any Personal Data that Company processes on behalf of Customer via the Services, as more particularly described in this DPA.

"Data Protection Laws" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"EU Data Protection Law" means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union).

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"Non-EU Data Protection Laws" means the California Consumer Privacy Act ("CCPA").

"SCCs" means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Company.

"Sensitive Data" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"Service Data" means any data relating to the Customer's use, support and/or operation of the Services.

"Sub-processor" means any processor engaged by Company to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties but shall exclude Company employees or consultants.

The terms “controller”, “data subject”, “processor” and “processing” shall have the meaning given to them under Data Protection Laws or if not defined thereunder, the GDPR, and “process”, “processes” and “processed” shall be interpreted accordingly.

2. Roles and Responsibilities.

2.1 Parties’ roles. If EU Data Protection Law applies to either party's processing of Customer Data, the parties acknowledge and agree that with regard to the processing of Customer Data, Customer is the controller and Company is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA.

2.2 Purpose limitation. Company shall process Customer Data only in accordance with Customer’s documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing (“Permitted Purposes”); provided that Company shall inform Customer if, in its opinion, Customer’s processing instructions infringe any law or regulation; in such event, Company is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation. The parties agree that the Agreement sets out Customer’s complete and final instructions to Company in relation to the processing of Customer Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 Prohibited data. Customer will not provide (or cause to be provided) any Sensitive Data to Company for processing under the Agreement, and Company will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 Customer compliance. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Customer Data and any processing instructions it issues to Company; (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Company to process Customer Data for the purposes described in the Agreement; (iii) if Customer is itself a data processor acting on behalf of a third-party data controller, Customer warrants to Company that Customer’s instructions and actions with respect to that Personal Data, including its appointment of Company as another data processor, have been authorized by the relevant data controller; (iv) that Customer will inform its Data Subjects as legally required: (a) about its use of data processors to process their Personal Data, including data processor; and (b) that their Personal Data may be processed outside of the European Economic Area; (v) that it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the processing of their Personal Data by Customer, and to give appropriate instructions to data processor in a timely manner; and (vi) that it shall respond in a reasonable time to enquiries from a data regulatory authority regarding the processing of relevant Personal Data by Customer. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any content created through the use of the Services.

2.5 Lawfulness of Customer's instructions. Customer will ensure that Company’s processing of the Customer Data in accordance with Customer’s instructions will not cause Company to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Company shall promptly notify Customer in writing, unless prohibited from doing so under EU Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates the GDPR or any UK implementation of the GDPR.

3. Sub-processing. Authorized Sub-processors. Customer agrees that Company may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Company and authorized by Customer are provided in Annex E and may be updated on Company’s website.

4. Security.

4.1 Security Measures. Company shall implement and maintain appropriate technical and organizational security measures (including the measures referred to in Article 32(1) of the GDPR) that are designed to protect Customer Data from Security Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with Company's security standards ("Security Measures").

4.2 Confidentiality of processing. Company shall ensure that any person who is authorized by Company to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality.

4.3 Updates to Security Measures. Customer is responsible for reviewing the information made available by Company relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Company may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

4.4 Security Incident response. Upon becoming aware of a Security Incident, Company shall: (i) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Company's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Company of any fault or liability with respect to the Security Incident.

4.5 Customer responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services.

5. Security Reports and Audits.

5.1 Audit rights. Company shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA and any audit rights granted by Data Protection Laws, by instructing Company to comply with the audit measures described in Section 5.2 below.

5.2 Company shall respond to all reasonable requests for information made by Customer to confirm Company's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to Company, provided that Customer shall not exercise this right more than once per calendar year.

6. International Transfers.

6.1 Data center locations. Customer acknowledges that Company may transfer and process Customer Data to and in the United States and anywhere else in the world where Company or its Sub-processors maintain data processing operations. Company shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws.

6.2 European Data transfers. To the extent that Company is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data"), the parties agree that Company makes available the mechanisms listed below:

- (a) SCCs: Company agrees to abide by and process EU Data in compliance with the SCCs, which are incorporated in full by reference and form an integral part of this DPA. For the purposes of the SCCs: (i) Company agrees that it is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may itself be an entity located outside the EU); (ii) Annexes A and B of this DPA shall replace Appendixes 1 and 2 of the SCCs, respectively; and (iii) Annex C shall form Appendix 3 of the SCCs. The parties further agree that the SCCs will apply to Customer Data that is transferred via the Services from Europe to outside Europe, either directly or via onward transfer, to any country or recipient: not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the EU Data Protection Law).

7. Return or Deletion of Data.

7.1 Deletion on termination. Upon termination or expiration of the Agreement, Company shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Company is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Company shall securely isolate, protect from any further processing and eventually delete in accordance with Company's deletion policies, except to the extent required by applicable law.

8. Data Subject Rights and Cooperation.

8.1 Data subject requests. Company shall, taking into account the nature of the processing, provide reasonable assistance to Customer to the extent possible to enable Customer to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made to Company directly, Company shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If Company is required to respond to such a request, Company shall promptly notify Customer and provide Customer with a copy of the request unless Company is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Company from responding to any data subject or data protection authority requests in relation to Personal Data for which Company is a controller.

8.2 Subpoenas and court orders. If a law enforcement agency sends Company a demand for Customer Data (for example, through a subpoena or court order), Company shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Company shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy, unless Company is legally prohibited from doing so.

8.3 Data protection impact assessment. To the extent required under applicable Data Protection Laws, Company shall (taking into account the nature of the processing and the information available to Company) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Company shall comply with the foregoing by: (i) complying with Section 5 (Security Reports and Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. Jurisdiction-Specific Terms.

To the extent Company processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex D, then the terms specified in Annex D with respect to the applicable jurisdiction(s) ("Jurisdiction-Specific Terms") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity

between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Company.

10. Limitation of Liability.

10.1 Each party's liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against Company under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement.

11.1 This DPA shall remain in effect for as long as Company carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7.1 above).

11.2 Regarding the subject matter of this DPA, in the event of any conflict between this DPA and any other written agreement between the parties (including the Agreement), this DPA will govern and control. Notwithstanding the foregoing, if there is any conflict between this DPA and a Business Associate Agreement applicable to any patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state laws, rules or regulations ("HIPAA Data"), then the BAA shall prevail to extent the conflict relates to such HIPAA Data.

11.3 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.4 Notwithstanding anything to the contrary in the Agreement (including this DPA), Company shall have a right to collect, use and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize and maintain the Services; (iii) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or (iv) as required by applicable law.

To the extent any such Service Data is considered Personal Data under Data Protection Laws, Company shall be responsible for and shall process such data in accordance with Company's Privacy Policy and Data Protection Laws. For the avoidance of doubt, this DPA shall not apply to Service Data.

11.6 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

11.7 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A – Details of Data Processing

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration of processing: Company will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(c) Purpose of processing: Company shall only process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Services in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Services; and (iii) processing to comply with any other reasonable instructions provided by Customer that are consistent with the terms of the Agreement.

(d) Nature of the processing: Processing conducted in connection with Company's provision of Services, as more particularly described in the Agreement.

(e) Types of Customer Data and categories of data subjects may include but is not limited to: The types of Customer Data and categories of data subjects are controlled by Customer in its sole discretion.

(f) Sensitive Data: Company does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Services.

(g) Processing Operations: Customer Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain and improve the Services provided to Customer pursuant to the Agreement; and/or
- Disclosures in accordance with the Agreement and/or as compelled by applicable law.

Annex B – Security Measures

Company takes all measures that are required under Article 32 of the General Data Protection Regulation. Company implements appropriate technical and organizational measures to protect the Personal Data made available from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

Company may change the implemented security measures on an ongoing basis, but when doing so, Company must make efforts to ensure that the changes overall do not result in a reduced level of security.

Company has determined the level of security on the basis of considerations concerning the expected categories of data subjects.

Company implements security measures, considering on average what is appropriate and the Parties therefore agree that in the mutual relationship the Customer is responsible for assessing whether the measures implemented are sufficient to reach a security level that matches the risk involved in the processing activities entrusted to Company.

Annex C

All defined terms used in this Annex C shall have the meaning given to them in the SCCs unless otherwise defined in this Annex.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "Agreement" shall have the meaning given to it in the DPA.

Clause 5(a): Suspension of data transfers and termination

1. The parties acknowledge that data importer may process the Personal Data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the Clauses.
3. If the data exporter intends to suspend the transfer of Personal Data and/or terminate these Clauses, it shall endeavor to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of Personal Data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their Personal Data.

Clause 5(f): Audit

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Security Reports and Audits) of the DPA.

Clause 5(j): Disclosure of sub-processor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.
3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

1. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, any PaaS Services Order Form or the Agreement, whether in contract, tort or under any other theory of liability, shall remain 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 this DPA, including all Annexes hereto. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by Company in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Company's liability under the Agreement as if it were liability to the Customer under the Agreement.

Clause 11: Onward sub-processing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.

Annex D - Jurisdiction-Specific Terms

Europe:

1. Objection to Sub-processors. Customer may object in writing to Company's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Company will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Services in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

California:

1. The definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "Personal Data" includes "Personal Information"; in each case as defined under CCPA.
2. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, or as otherwise may be permitted for "service providers" under the CCPA.
3. Company's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer's rights under the CCPA.
4. Notwithstanding any use restriction contained elsewhere in this DPA, Company shall process Customer Data only to perform the Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law.
5. Company may de-identify or aggregate Customer Data as part of performing the Services specified in this DPA and the Agreement.

Annex E – Sub-processors

Company uses certain Sub-processors and subcontractors to assist it in providing the Services as described in the Agreement. Capitalized terms used herein shall have the same meaning as defined in the Agreement.

What is a Sub-processor:

A Sub-processor is a third party data processor utilized by Company in the delivery of its Services, who has or potentially will have access to or will process Customer Data (including Personal Data) or who may receive Personal Data from Customer as part of Company providing the Services. Company engages different types of Sub-processors to perform various functions as explained in the tables below. Note that third party Services linked to within the Services are not considered Company Sub-processors. Such Services are provided subject to the terms of service and privacy policies applicable to such Services.

Contractual Safeguards:

Company requires its Sub-processors to satisfy equivalent obligations as those required from Company (as a Data Processor) as set forth in Company's Data Processing Addendum ("DPA"), including but not limited to the requirements to:

- process Personal Data in accordance with data controller's (i.e. Customer's) documented instructions (as communicated in writing to the relevant Sub-processor by Company);
- implement and maintain appropriate technical and organizational measures (including measures consistent with those to which Company is contractually committed to adhere insofar as they are equally relevant to the Sub-processor's processing of Personal Data on Company's behalf); and
- promptly inform Company about any security breach.

This policy does not give Customer any additional rights or remedies and should not be construed as a binding agreement. The information herein is only provided to illustrate Company's engagement process for Sub-processors as well as to provide the actual list of third party Sub-processors used by Company as of the date of this policy (which Company may use in the delivery and support of the Services).

Infrastructure Sub-processors:

Company utilizes certain cloud service providers to host the Services, to provide Company with certain services related to the provisioning of the Services, including storing certain data relating to the Services.

Entity	Purpose	Entity Country
Amazon Web Subscription Services	Cloud Service Provider	United States
Databricks	Cloud Service Provider	United States

Service-specific Sub-processors:

Company works with certain third parties to provide specific functionality within the Services.

Entity	Purpose	Applicable Services	Entity Country

Okta	Company utilizes Okta to manage and secure user authentication on Tecton's application.	Company Support	United States
PagerDuty	Company utilizes PagerDuty to provide emergency ticket routing.	Company Support	United States
Slack	Company offers the use of Slack to provide certain support offerings.	Company Support	United States
Google G Suite	Company utilizes Google G Suite for communication, storage, productivity, and collaboration.	Company Support	United States
Jira	Company utilizes Jira as a work management tool.	Company Support	United States
Chronosphere	Company utilizes Chronosphere as a monitoring platform.	Company Support	United States