

DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its Annexes (“DPA”) has been entered into on **[insert date]** by and between **APERIA TECHNOLOGIES, INC.**, a corporation organized under the laws of the state of **[state]** (“Company”), and **[insert data processor entity name]**, a **[insert form of legal entity]** organized under the laws of **[insert jurisdiction of formation]** (“Supplier”) to address how the Parties agree to process personal data. Company and Supplier are each a “Party” and together the “Parties.”

Background

The Parties entered into a **[description of Agreement]**, dated **[insert date]** (“Service Agreement”).

The Parties wish to supplement the terms of the Service Agreement to ensure that the Processing of Personal Information by Supplier in connection with the Service Agreement is in compliance with Data Protection Laws.

This DPA governs any Processing of Personal Information by Supplier in connection with the Services, as defined in the Service Agreement, and supplements the terms of the Service Agreement applicable to the Services, except where Company and Supplier have entered into another DPA applicable to certain of the Services.

In the event of any conflict or inconsistency between this DPA and the Service Agreement, this DPA will control.

The term of this DPA will follow the term of the Service Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Service Agreement.

The Parties agree:

1. **Data Protection.** Supplier shall comply with Data Protection Laws in connection with performing the Services and its obligations under the Service Agreement and this DPA.
2. **Data Processing Activities.** In relation to Personal Information Processed by Supplier in connection with the Service Agreement, the subject-matter, nature, purpose and duration of the Processing, the data subjects concerned and the categories of Personal Information are specified in Annex 1.
3. **Supplier Obligations.** When Processing Personal Information on behalf of Company in connection with the Service Agreement, Supplier shall:
 - 3.1. only Process Personal Information on Company’s documented instructions, including Supplier performing its obligations under, and in accordance with, the Service Agreement and this DPA, unless required otherwise by applicable Law. In that case, Supplier shall, inform Company of that legal requirement before commencing the Processing, unless prohibited by that applicable Law, shall use its

best efforts to limit the nature and scope of any required disclosure and shall only disclose the minimum amount of Personal Information necessary to comply with that applicable Law.

- 3.2. ensure that at all times Personal Information is Processed only to the minimum extent necessary to accomplish the purpose of the Processing permitted under this DPA and Service Agreement.
- 3.3. immediately inform Company if Supplier is of the opinion that an instruction of Company regarding Processing Personal Information infringes Data Protection Law.
- 3.4. ensure that (i) Supplier limits access to Personal Information to Supplier's personnel who need access to Personal Information for the purposes of performing the Services under the Service Agreement and (ii) Supplier's personnel who have access to Personal Information only Process the Personal Information, as permitted under this DPA and Service Agreement, and are subject to confidentiality obligations that are at least as protective of Personal Information as Supplier's obligations under this DPA and the Service Agreement.
- 3.5. not disclose or transfer Personal Information to any third party, or otherwise engage any agent or subcontractor in any Processing under the Service Agreement, unless (i) Company has provided its prior written consent, (ii) Supplier has carried out reasonable due diligence to ensure the third party is capable of providing the level of protection of Personal Information required under this DPA and the Service Agreement, (iii) the third party has entered into a written agreement including terms that are at least as protective of Personal Information as the obligations set out in this DPA and the Service Agreement and (iv) the third party meets the requirements of Data Protection Law. A current list of subcontractors, if any, for which Company has given its prior written consent as of the date of this DPA is specified in Annex 1.
- 3.6. be fully liable for all acts or omissions of its employees, affiliates, agents, subcontractors and other representatives in the same manner as for its own acts or omissions.
- 3.7. implement and maintain reasonable and appropriate written information security and privacy programs, which programs shall incorporate physical, technical and organizational measures that are commensurate with the nature of Personal Information Processed under the Service Agreement, that meet or exceed good industry practices (or such higher standard as may be required in Annex 1) and that are adequate to reasonably protect against a Personal Data Breach, including training of all personnel responsible for Processing Personal Information of the requirements of this DPA and the Service Agreement, such measures described in Annex 1 and to the extent not otherwise addressed in Annex 1 and as appropriate:
 - a) the pseudonymisation and encryption of Personal Information;

- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and
- e) the ability to establish timely (in any event within 72 hours of occurrence) if a Personal Data Breach has occurred.

3.8. in the event of an actual or reasonably suspected Personal Data Breach of Personal Information within the custody or control of Supplier (a “**Supplier Personal Data Breach**”), a breach of Data Protection Laws by Supplier or any other breach of this DPA or the Service Agreement by Supplier, at Supplier’s sole cost and expense, (i) notify Company without undue delay (and in any event, within 24 hours of becoming aware of an actual or suspected Supplier Personal Data Breach); (ii) undertake an appropriate investigation and all remediation efforts necessary to rectify and prevent a recurrence of such Supplier Personal Data Breach, breach of Data Protection Laws or other breach of this DPA or the Service Agreement and for the Parties to comply with Data Protection Law; and (iii) promptly provide Company with all information Company deems necessary to enable Company to comply with applicable requirements under Data Protection Law, including with respect to record keeping and reporting, and all other information Company may reasonably request regarding a Supplier Personal Data Breach, breach of Data Protection Laws or other breach of this DPA or the Service Agreement. In the case of an actual or suspected Supplier Personal Data Breach involving Company’s Personal Information, and without limiting any of Supplier’s other obligations, as part of the remediation efforts, upon Company’s request, Supplier shall provide notification to all data subjects whose Personal Information may have been affected, with content required under Data Protection Laws and satisfactory to Company, or provide Company with all assistance and information necessary to enable Company to provide notification to any and all data subjects whose Personal information may have been affected, as Company deems appropriate. Supplier is solely responsible for the costs and expenses of either Party for any such notification to data subjects, whether the notice was given by Supplier or Company. Except for Supplier’s attorneys and consultants engaged with respect to the investigation or remediation of a Supplier Personal Data Breach involving Company Personal Information or breach of this DPA or the Service Agreement, other third parties involved in a Supplier Personal Data Breach involving Company Personal Information engaged with respect to the investigation or remediation of that Supplier Personal Data Breach and Supplier’s insurers, the Supplier may not provide any third parties with any information regarding an actual or suspected Supplier Personal Data Breach involving Company Personal Information or other breach of this DPA or the Service Agreement, without Company’s prior written

consent, unless otherwise required by applicable Law. If that applicable Law requires Supplier to provide a third party with any information regarding an actual or suspected Supplier Personal Data Breach involving Company's Personal Information or other breach of this DPA or the Service Agreement, the Supplier shall promptly notify Company (in any event, within 24 hours) of each such communication with a third party, describing the content of the communication, and sending Company a copy of all written correspondence, unless prohibited under that Law. For the avoidance of doubt, Personal Information in the custody or control of Supplier includes any Personal Information in the custody or control of any of Supplier's affiliates or Supplier's or any of its affiliates' agents, subcontractors or other representatives.

- 3.9. promptly notify Company without undue delay, and in any event, within 24 hours, of:
 - (i) any inquiry, request for information from or complaint by a competent data protection or other regulatory authority, relating to Personal Information that Supplier Processes in connection with the Service Agreement; and
 - (ii) any complaint, inquiry or request by a data subject relating to the Personal Information Supplier Processes in connection with the Service Agreement, including any request to exercise rights under Data Protection Laws or Company's or Supplier's privacy policy, such as to access, rectify, amend, correct, share, delete or cease Processing his or her Personal Information.
- 3.10. provide all assistance, including implementing appropriate technical and organizational measures, and information Company may reasonably request (i) for Company to comply with its obligations under Data Protection Laws (including in responding to requests from data subjects exercising their rights under Data Protection Law, conducting data protection impact assessments, consulting with competent data protection and other regulatory authorities, notifying relevant competent data protection and other regulatory authorities and data subjects of Personal Data Breaches, and ensuring Personal Information protection) and otherwise investigate and address any other request, complaint, inquiry or concern by data subjects or competent data protection or other regulatory authorities and (ii) for Supplier to demonstrate Supplier's compliance with the provisions of this DPA or the Service Agreement and compliance with Data Protection Law.
- 3.11. on Company's request or at the expiration or earlier termination of the Service Agreement or a Statement of Work to which the Personal Information is applicable, promptly delete or return, at Company's option, all Personal Information Processed, unless required otherwise by applicable Law. In that case, Supplier may retain one copy of the Personal Information required to be retained under applicable Law, until 30 days after that period for retaining Personal Information required under applicable Law ends, and Supplier will continue to comply with this DPA or the Service Agreement with respect to any Personal Information Supplier retains and will only Process that Personal Information as required by that applicable Law.

Supplier shall delete or return the Personal Information by such means and, in the case of returning Personal Information, in such format, as Company reasonably requests.

- 3.12. maintain the accuracy and integrity of Personal Information that it Processes on behalf of Company.
- 3.13. maintain all records necessary to be able to demonstrate that Personal Information was only Processed in accordance with applicable notices, consents authorizations and rights and as permitted under this DPA or the Service Agreement and for each of Company and Supplier to comply with Data Protection Law.
- 3.14. upon Company's request, allow for and contribute to audits by Company or another auditor mandated by Company of Supplier's compliance with this DPA or the Service Agreement and of Supplier's privacy and information security programs, and have a third-party auditor, reasonably acceptable to Company, conduct an audit of Supplier's privacy and information security programs.
- 3.15. to the extent, in connection with the Service Agreement, Supplier is to Process Personal Information related to:
 - a) individuals residing in the European Economic Area ("EEA"), Switzerland or Serbia, Process that Personal Information only within the European Economic Area, Switzerland or Serbia, respectively, except upon Company's prior written consent and where permitted under applicable Data Protection Law, and upon doing all things Company determines are necessary, to comply with Data Protection Law, including entering the Standard Contractual Clauses.
 - b) individuals residing in countries outside of the EEA, Switzerland or Serbia that have restrictions on cross-border transfer of Personal Information, Process that Personal Information only within that country, except upon Company's prior written consent and where permitted under applicable Data Protection Law, and upon doing all things Company determines are necessary, to comply with Data Protection Law.
- 3.16. not change the location where any Personal Information is Processed under this DPA or the Service Agreement, except with Company's prior written consent and as permitted by Data Protection Law.
- 3.17. as required by applicable Data Protection Law, and upon Company's request, provide notice to, and obtain a consent from, any data subject whose Personal Information is collected by or on behalf of Supplier in connection with the Service Agreement. Supplier will use forms of notice and consent, and provide and obtain any such notice and consent in a manner and at the times that are satisfactory to Company and meet the requirements of applicable Law.

- 3.18. Except for changes made consistent with meeting industry practice or Data Protection Law, Supplier shall maintain in effect and consistently apply, Supplier's privacy and data security practices disclosed to Company in connection with any due diligence Company most recently conducted on those practices in connection with the Service Agreement. Supply represents and warrants that all responses provided by Supplier in any such due diligence are true, accurate and complete when made and if later, as of the effective date of the Service Agreement. Supplier shall promptly notify Company of all material changes to Supplier's privacy and data security practices.
- 3.19. promptly provide to Company the minimum information necessary regarding individuals who have opted out of receiving future communications from Company or who have opted out of any other use or disclosure of Personal Information by Company, including the relevant contact Information and the specific nature of the request, to enable Company to observe such opt-outs in compliance with applicable Law. Supplier also agrees to reflect in its data those individuals who have opted out of receiving communications immediately upon receipt of such information, whether received directly from the individual or from Company.
4. Remediation. Without limiting any of Company's rights or entitlements, or Supplier's obligations, under the Service Agreement or otherwise, the Parties agree that Company will be entitled to recover from Supplier any losses, damages, fines, costs, or expenses (including legal expenses and disbursements) incurred by Company or its affiliates or their respective officers, directors, employees, contractors, temporary workers, subcontractors, agents or other representatives resulting from (i) a Supplier Personal Data Breach in relation to Personal Information Processed by Supplier in connection with the Service Agreement, (ii) breach of Data Protection Laws by Supplier in connection with the Service Agreement, or (iii) a breach of any provision of this DPA or the Service Agreement, and such amounts shall be deemed direct losses and not subject to any limitations or exclusions of liability (whether in the Service Agreement or otherwise).
5. Definitions and Interpretation. In this DPA, the following definitions apply:
- "California Personal Information" means Personal Data that is subject to the protection of the CCPA.
 - "CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or "CPRA").
 - "Consumer", "Business", "Sell", "Service Provider", and "Share" will have the meanings given to them in the CCPA.
 - "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

- “Data Privacy Framework” means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.
- “Data Privacy Framework Principles” means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded or replaced.
- “Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Service Agreement, including without limitation European Data Protection Laws, the CCPA and other applicable U.S. federal and state privacy laws, and the data protection and privacy laws of Australia, Singapore, and Japan, in each case as amended, repealed, consolidated or replaced from time to time.
- “Data Subject” means the individual to whom Personal Data relates.
- “Europe” means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.
- “European Data” means Personal Data that is subject to the protection of European Data Protection Laws.
- “European Data Protection Laws” means data protection laws applicable in 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; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”); and (iv) Swiss Federal Data Protection Act and its Ordinance (“Swiss DPA”); in each case, as may be amended, superseded or replaced.
- “Law” means any applicable laws, ordinances, rules, regulations and lawful orders of any public authority (including, and by way of example only, interpretations and decisions of, or agreements with, any competent regulatory authority) to which either Party, as applicable, is subject in connection with the Service Agreement;
- “Personal Information” or “Personal Data” means any data relating to an identified or identifiable individual, including data that identifies an individual or that could be used to identify, locate, track, or contact an individual. Personal Information includes both directly identifiable information such as a name, identification number or unique job title, and indirectly identifiable information such as date of birth, unique mobile or wearable device

identifier, telephone number, key-coded data and online identifiers such as IP addresses, and includes any data that constitutes “personal data” under the GDPR.

- “Personal Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored or otherwise Processed.
 - “Controller”, “Data Subject” and “Processing” each have the meaning given in the European Union General Data Protection Regulation 2016/679 (the “GDPR”), irrespective of whether GDPR applies in any particular context; “Standard Contractual Clauses” means the standard contractual clauses approved by European Commission Decision 2021/914 of 4 June 2021 currently found at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914>, or as may be amended or replaced from time to time by European Commission decisions or other applicable Data Protection Laws.
 - “UK Addendum” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>, as may be amended, superseded, or replaced.
6. In the event that the definitions in this DPA are inconsistent with the definitions given similar terms or concepts under Data Protection Laws, then the definition given any such similar term or concept under that applicable Data Protection Laws shall prevail to the extent of the inconsistency, so long as such inconsistency results in a broader definition of such term or concept. The words “include” and “including” shall be construed to mean including without limitation. In connection with the Services under the Service Agreement, Supplier may Process Personal Information of one or more of Company’s affiliates. In such event, any of those Company affiliates shall be considered a “controller” of Personal Information and a third party beneficiary of this DPA and entitled to rely upon and enforce all rights and protections afforded Company under this DPA, whether or not that affiliate is named as a party to the Service Agreement or this DPA. This DPA is hereby incorporated into and forms part of the Service Agreement. In the event and to the extent of any conflict between the terms of the Service Agreement and this DPA, the terms of this DPA will prevail, except if the terms of the Service Agreement are more protective of Company Personal Information, in which case the more protective terms of that Service Agreement will prevail. In the event and to the extent of any conflict between the terms of this DPA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail. Except as expressly amended herein, the terms of the Service Agreement will remain in full force and effect. If this DPA is drafted in English and a foreign language, in the case of differences between the text in English and the text in the foreign language, the text in English shall prevail. Section and other headings in this DPA are for convenience of reference only and shall not constitute a part of or otherwise affect the meaning or interpretation of this DPA. Annexes and appendices to this DPA shall be deemed to be an integral part of this DPA to the same extent as if they had been set forth verbatim in this DPA. The provisions of this DPA are severable. If any phrase, clause or

provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

7. Additional Provisions for California Personal Information.

a. Scope. The ‘Additional Provisions for California Personal Information’ section of this DPA will apply only with respect to California Personal Information.

b. Roles of the Parties. When processing California Personal Information in accordance with Company Instructions, the parties acknowledge and agree that Company is a Business and Supplier is a Service Provider for the purposes of the CCPA.

c. Responsibilities. Service Provider certifies that Service Provider will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Service Agreement (the “**Business Purpose**”) or as otherwise permitted by the CCPA, including as described in the Company Privacy Policy. Further, Service Provider certifies that Service Provider (i) will not Sell or Share California Personal Information; (ii) will not Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; and (iii) will not combine the California Personal Information included in Customer Data, as defined in the CCPA, with personal information that Service Provider collects or receives from another source (other than information received from another source in connection with obligations as a Service Provider under the Service Agreement).

d. Compliance. Service Provider will (i) comply with obligations applicable to it as a Service Provider under the CCPA and (ii) provide California Personal Information with the same level of privacy protection as is required by the CCPA. Service Provider will notify Company if Service Provider makes a determination that Service Provider can no longer meet its obligations as a Service Provider under the CCPA.

e. CCPA Audits. Service Provider will have the right to take reasonable and appropriate steps to help ensure that it uses California Personal Information in a manner consistent with Customer’s obligations under the CCPA. Upon notice, Company will have the right to take reasonable and appropriate steps in accordance with the Service Agreement to stop and remediate unauthorized use of California Personal Information.

f. Not a Sale. The Parties acknowledge and agree that the disclosure of California Personal Information by the Customer to Supplier does not form part of any monetary or other valuable consideration exchanged between the parties.

8. Counterparts. This DPA may be entered into in any number of counterparts, all of which together will constitute one and the same instrument. Any Party may enter into this DPA by executing such counterpart.

9. Entire Agreement. This DPA constitutes the entire agreement between the Parties with respect to the subject of this DPA and (to the extent permissible by law) supersedes all prior representations or oral or written agreements between the Parties with respect to that

subject matter, provided that nothing in this DPA will operate to supersede any representations, terms or provisions in the Service Agreement or other prior written agreement between Company and Supplier that are more protective of Company Personal Information than as may be set out in this DPA and neither Party is attempting to exclude any liability for fraudulent statements.

10. Governing law and Jurisdiction. The governing law and jurisdiction provisions of the Service Agreement will apply to this DPA.
11. Notice. Notices given under this DPA (each a “**Notice**”) shall be in writing. Notices given under this DPA shall be given in accordance with the notice provisions of the applicable Service Agreement, together with copy(ies) sent to the Company by email, to the email address(es) below, marked with a subject line of “DPA Notice from Supplier” or in the case of a Personal Data Breach “Urgent: Personal Data Breach Notice”:

If to Company: [email](#)

APERIA TECHNOLOGIES, INC.

Signed for and on behalf of *[insert full name of Supplier entity]*:

By: _____

By: _____

Name:

Title:

Date: _____

Date: _____

ANNEX 1 – DESCRIPTION OF PROCESSING

A. List of Parties

Data exporter:

Name: The Customer, as defined in the Terms of Service (on behalf of itself and Permitted Affiliates)

Address: The Customer's address, as set out in the Order Form

Contact person's name, position and contact details: The Customer's contact details, as set out in the Order Form

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Services under the Terms of Service

Role (controller/processor): Controller (either as the Controller; or acting in the capacity of a Controller, as a Processor, on behalf of another Controller)

Data importer:

Name: Aperia Technologies, Inc.

Address: **[address]**

Contact person's name, position and contact details: **[information]**

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the Services under the Terms of Service

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

Supplier may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by Supplier in Supplier's sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Supplier's contacts and other end users including Supplier's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Supplier's end users.

Categories of Personal Data Transferred

Supplier may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by Supplier in Supplier's sole discretion, and which may include but is not limited to the following categories of Personal Data:

1. Contact Information (as defined in the General Terms).
2. Any other Personal Data submitted by, sent to, or received by Supplier, or Supplier's end users, via the Subscription Service.
3. Sensitive Data transferred and applied restrictions or safeguards

The Parties do not anticipate the transfer of sensitive data.

Frequency of the transfer

Continuous

Nature of the Processing

Personal Data will be Processed in accordance with the Service Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to Supplier; and/or
2. Disclosure in accordance with the Service Agreement (including this DPA) and/or as compelled by applicable laws.

Purpose of the transfer and further processing

We will Process Personal Data as necessary to provide the Subscription Services pursuant to the Service Agreement, as further specified in the Order Form, and as further instructed by Supplier in Supplier's use of the Subscription Services.

Period for which Personal Data will be retained

Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Service Agreement, unless otherwise agreed in writing.

C. Current List of Subcontractors

Appendix 1
to
Annex 1 of Data Processing Agreement

Information Technology Security Measures

- 1. Network Security** - Supplier shall maintain network security policies, procedures, and systems and shall perform network security and activities consistent with best practices in Supplier's industry but that, at a minimum, include but are not limited to: network firewall provisioning, intrusion detection, and regular (but in no event less frequently than annually) vulnerability assessments. In no event shall the foregoing as applied to the Personal Information of the Company be any less stringent and protective than those applied by Supplier to the protection of its own data and systems of a like or similar nature.
- 2. Application Security** - Supplier shall provide, maintain and support any of its software and systems provided or used in connection with the services or products under the Service Agreement and subsequent updates, upgrades, and bug fixes such that they are and remain secure from vulnerabilities, utilizing recognized and comparable industry practices or standards as set forth in paragraph 9 below.
- 3. Data Security** - Without limiting Supplier's confidentiality obligations or other obligations to protect data and other information of Company or its Affiliates, including without limitation, any Personal Information, under the Service Agreement or this DPA, Supplier shall store all Personal Information in accordance with industry best practices and in compliance with all applicable Laws, and use security measures, including, but not limited to, encryption and firewalls, to protect such Personal Information from unauthorized disclosure or use. Such measures shall be no less rigorous than those measures maintained by Supplier for its own data of a similar nature. When Supplier stores Personal Information in a third-party's offsite facility, Supplier must have complied with the terms of this DPA related to disclosing Personal Information to third parties or otherwise subcontracting services or products to third parties and shall only use a third party's offsite storage facility that is otherwise reasonably acceptable to Company, without limiting the foregoing, the facility of a third party that is in full compliance with all of the provisions of this Appendix.
- 4. Data storage** - Any and all Personal Information will be stored, processed, and maintained solely on designated Supplier computing and storage resources, and that no Personal Information will at any time be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of the Supplier's designated backup and recovery processes and encrypted

in accordance with paragraph 6 below. Supplier shall store all backup Personal Information as part of its designated backup and recovery processes.

5. **Data Transmission** - Any and all electronic transmission or exchange of Personal Information with Company and/or any third parties shall take place via secure means (using HTTPS or SFTP or equivalent) and solely in accordance with paragraph 6 below.
6. **Data Encryption** - Supplier agrees that any and all Personal Information stored on any portable or laptop computing device or any portable storage medium, including all company backup data, shall be kept in encrypted form, using a commercially supported encryption solution. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption.
7. **Data Re-Use** –Except as required to provide the services or products under the Service Agreement or as otherwise permitted under this DPA, Supplier shall not distribute, repurpose or share across other applications, environments, or business units of Supplier any Personal Information.
8. **Security Breach Notification** - In the event of a personal data breach or breach of any of Supplier’s security obligations, then in addition to its obligations under the Service Agreement or the DPA, Supplier shall notify Company of such an event within 24 hours of discovery by telephone and e-mail at the following phone number and email address:
Security Breach Notice Telephone No.: **[number]**

Security Breach Notice Email: **[email]**

Data Exporter

APERIA TECHNOLOGIES, INC.

By: _____

Date: _____

Data Importer

Signed for and on behalf of *[insert full name of Supplier entity]*:

By: _____

Name:

Title:

Date: _____

Appendix 1 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The physical, technical and organizational measures that are commensurate with the nature of personal information processed, that meet or exceed good industry practices [(or such higher standard as may be required in Annex 1 to the DPA referenced below)] and that are adequate to reasonably protect against a Personal Data Breach, implemented by the data importer, as required in accordance with the terms of that certain [Data Processing Agreement] between data exporter and data importer dated [insert date] (the “DPA”), including training of all personnel responsible for processing personal information of the requirements of the DPA, such measures described Annex 1 to the DPA and, to the extent not otherwise addressed in Annex 1 to the DPA, as appropriate:

- i. the pseudonymisation and encryption of Personal Information;
- ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- iii. the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident;
- iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and,
- v. the ability to establish timely (in any event within 72 hours of occurrence) if a Personal Data Breach has occurred.