aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Last updated: September 18, 2023

This Data Processing Addendum (**"DPA"**) forms part of the Master Services Agreement or other written or electronic agreement between Aperian Global, Inc. and Customer (the **"Agreement"**) for the purchase of online services from Aperian (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as **"Services"** or **"Aperian Services"**) 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 and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Aperian 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 Aperian Services to Customer pursuant to the Agreement, Aperian will 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. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules. This DPA supersedes all prior and contemporaneous data processing agreements or data processing terms in any agreements, proposals or representations, written or oral, concerning the Processing of Personal Data.

1. **Definitions**
    - **"Affiliates"** means any entity under the control of a Party where "control" means ownership of or the right to control greater than 50% of the voting securities of such entity.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **"CCPA"** means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq.) and its implementing regulations, as may be amended, superseded or replaced from time to time.
- **"Data Protection Laws"** means all data protection and privacy laws, regulations and secondary legislation applicable to the respective Party in its role in the processing of Customer Personal Data under the Agreement, including in particular and to the extent applicable European Data Protection Laws and the CCPA, as may be amended, superseded or replaced from time to time.
- **"Europe"** means for the purposes of this DPA, the European Economic Area and/or its member states (**"EEA"**), the United Kingdom (**"UK"**) and/or Switzerland.
- **"European Data Protection Laws"** means (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) (**"EU 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); (iv) in respect of the United Kingdom, the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the **"UK GDPR"**) and the Data Protection Act 2018 (together the **"UK Data Protection Laws"**); (v) the Swiss Federal Data Protection Act (**"Swiss DPA"**); and (vi) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii) (iv) or (v); in each case as may be amended or superseded from time to time;
- **"Customer Personal Data"** means any information which is protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Laws that Aperian processes on behalf of Customer under the Agreement, as more particularly described in **Annex A**.
- **"Permitted Affiliate"** means any Affiliate of Customer which: (i) is subject to Data Protection Laws and is a controller or business (as applicable) with respect to the Customer Personal Data; and (ii) is permitted to use the Services pursuant to the Agreement, but has not signed its own Order Form with Aperian and is not a "Customer" as defined under the Agreement.
- **"Privacy Shield"** means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield self-certification programs operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on 11 January 2017 respectively (as amended, superseded or replaced from time to time).

- **"Privacy Shield Principles"** means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 (as amended, superseded, or replaced from time to time).
- **"Restricted Transfer"** means a transfer (directly or via onward transfer) of Customer Personal Data that is subject to European Data Protection Laws to a country outside Europe which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).
- **"Security Incident"** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed by Aperian Global under this DPA. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- **"Sensitive Data"** means any information which is protected as "sensitive data", "special category data", "sensitive information", "sensitive personal information" or similar term under Data Protection Laws, including, but not limited to, (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences; (ii) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (**"PCI DSS"**); and (iii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (**"HIPAA"**).
- **"Standard Contractual Clauses"** or **"SCCs"** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
- **"Sub-processor"** means any third party that has access to Customer Personal Data and which is engaged by Aperian Global to assist in fulfilling its obligations with respect to providing the Services under the Agreement.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Sub-processor's may include Aperian Affiliates but shall exclude Aperian employees, contractors and consultants.

- **"UK Addendum"** means the International Data Transfer Addendum to the SCCs (version B1.0) issued by Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as it is revised under Section 18 therein; as may be amended or superseded from time to time.
- The lower case terms **"controller"**, **"personal data" "processor"**, **"process"**, **"processing"** and **"data subject"** have the meanings given to them in applicable Data Protection Laws or if not defined therein, the EU GDPR, and the terms "business", "consumer", "sale," (including the terms "sell," "selling," "sold," and other variations thereof) and **"service provider"** has the meaning set forth in the CCPA.

2. **Scope and Applicability of this DPA**
   - This DPA only applies where and only to the extent Aperian processes Customer Personal Data on behalf of Customer that is subject to Data Protection Laws as a (i) processor (for the purposes of European Data Protection Laws) or (ii) service provider (for the purposes of the CCPA), in the course of providing the Services pursuant to the Agreement. Each party shall process Customer Personal Data under this DPA in accordance with and as permitted by the Agreement and Data Protection Laws.
   - Any processing of Customer Personal Data under the Agreement shall be performed in accordance with applicable Data Protection Laws. However, Aperian is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that is not generally applicable to Aperian.
3. **Processing of Customer Personal Data**
   - **Permitted Purposes.** Aperian shall process Customer Personal Data in accordance with Customer's documented lawful instructions, except where required by applicable law(s). For these purposes, Customer instructs Aperian to process Customer Personal Data for the following purposes: (a) to perform any steps necessary for the performance of the Agreement; (b) to respond to any technical problems or Customer queries and ensure the proper working of the Services, (c) to provide, maintain and improve the Services provided to Customer in accordance with the Agreement; (d) processing initiated by end users in their use of the Services; (e) to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement (including this DPA); (f) to detect, prevent, and investigate Security Incidents, fraud, spam, or unlawful use of the Services, and (g) to comply with Aperian's legal obligations under applicable

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

law, including Data Protection Laws (collectively and individually the **"Permitted Purpose"**).

- **Processing Instructions.** The Parties agree that the Agreement (including this DPA), and Customer's use of the Services in accordance with the Agreement, set out Customer's complete and final processing instructions and any processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Aperian. Customer shall ensure its instructions are lawful and that the processing of Customer Personal Data in accordance with such instructions will not violate Data Protection Laws.
- **Customer Responsibilities.** Customer is responsible for determining whether the Services are appropriate for the storage and processing of Customer Personal Data under Data Protection Laws. Customer further agrees that: (a) it will comply with its obligations under Data Protection Laws regarding its use of the Services and the processing of Customer Personal Data; (b) it is responsible for the accuracy, quality and legality of the Customer Personal Data; (c) it has provided notice and obtained all consents, permissions and rights necessary for Aperian and its Sub-processors to lawfully process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA); (d) it will notify Aperian if it is unable to comply with its obligations under Data Protection Laws or its processing instructions will cause Aperian or its Sub-processors to be in breach of Data Protection Laws.
- **Sensitive Data.** The types of Customer Personal Data processed by Aperian are determined and controlled by the Customer in its sole discretion. Aperian does not intentionally collect any Sensitive Data in connection with the Services. Customer acknowledges that the Services are not designed to comply with data protection requirements that apply to Sensitive Data. In particular, but without limitation, Customer acknowledges that Aperian is not a business associate or subcontractor (as those terms are defined in HIPAA) or a payment card processor and that the Services are neither HIPAA nor PCI DSS compliant. Aperian will have no liability under this Agreement for Sensitive Data, notwithstanding anything to the contrary herein.
- **Aggregate Data.** Notwithstanding the foregoing or anything to the contrary in the Agreement, Customer acknowledges that Aperian Global and its Affiliates shall have a right to collect and create anonymized, aggregate and/or de-identified information (as defined by Data Protection Laws) for its own legitimate business purposes.

4. **Sub-processors**
   - **Approved Sub-processors.** Customer acknowledges and agrees that Aperian Global may engage Sub-processors in order to provide the Services. Customer

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

specifically authorizes the engagement of those Sub-processors listed at https://aperian.com/subprocessor-list (or such other successor URL notified to Customer from time to time) and **Annex C** (**"Sub-processor List"**). Aperian will restrict Sub-processors' access to Customer Personal Data to what is necessary to assist Aperian in providing or maintaining the Services and will remain responsible for any acts or omissions of Sub-processors to the extent they cause Aperian to breach its obligations under this DPA.

5. **Security**
    - **Security Measures.** Aperian shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and preserve the security and confidentiality of Customer Personal Data, in accordance with the measures described in **Annex B** (**"Security Measures"**). Customer acknowledges that the Security Measures are subject to technical progress and development and that Aperian may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.
    - **Access and Confidentiality.** Aperian restricts its personnel from processing Customer Personal Data without authorization and shall ensure that any person who is authorized by Aperian to process Customer Personal Data is under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
    - **Customer Responsibilities.** Notwithstanding the above, Customer is responsible for reviewing the information made available by Aperian relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Law. Customer further agrees that Customer is responsible for its secure use of the Services, including securing its account authentication credentials Customer and taking any appropriate steps to backup any Customer Personal Data processed in connection with the Services.
    - **Security Incidents.** Upon becoming aware of a Security Incident, Aperian shall notify Customer without undue delay and, where feasible, within 48 hours. Aperian shall provide Customer with timely information relating to the Security Incident as it becomes known or is reasonably requested by Customer to fulfill its obligations under Data Protection Laws. Aperian will also take reasonable steps to contain, investigate, and mitigate any Security Incident.
6. **Audits**
    - **Security Audits.** On written request from Customer, Aperian shall provide written responses (which may include audit report summaries/extracts) to all

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

reasonable requests for information made by Customer related to its processing of Customer Personal Data necessary to confirm Aperian's compliance with this DPA, provided that Customer shall not exercise this right more than once in any 12 month rolling period. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority, or Aperian has experienced a Security Incident, or on another reasonably similar basis. Nothing herein shall be construed to require Aperian to provide: (i) trade secrets or any proprietary information; (ii) any information that would violate Aperian's confidentiality obligations, contractual obligations, or applicable law; or (iii) any information, the disclosure of which could threaten, compromise, or otherwise put at risk the security, confidentiality, or integrity of Aperian's infrastructure, networks, systems, or data.

7. **International Transfers**
   Customer acknowledges and agrees that Aperian may transfer and process Customer Personal Data to and in the United States and the other locations in which Aperian, its Affiliates or its Sub-processors maintain data processing operations as more particularly described in the Sub-Processor List. Aperian shall ensure that such transfers are made in compliance with Data Protection Laws and this DPA.
8. **Deletion of Customer Personal Data**
   Within six (6) months upon termination or expiry of the Agreement, Aperian will delete all Customer Personal Data in its possession or control unless instructed otherwise by Customer upon termination and in writing. This requirement shall not apply to the extent Aperian is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data archived on back-up systems, which data Aperian shall securely isolate and protect from any further processing (to the extent permitted by applicable law).
9. **Cooperation**
   - **Data subject requests.** To the extent that Customer is unable to independently access the relevant Customer Personal Data within the Services, Aperian shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer in responding to any requests from individuals relating to the processing of Customer Personal Data under the Agreement. In the event that any such request is made to Aperian directly, Aperian shall promptly notify Customer and shall not respond to the request directly without Customer's prior authorization, unless legally compelled to do so.
   - **Law enforcement requests.** If a law enforcement agency sends Aperian a demand for Customer Personal Data (for example, through a subpoena or

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

court order), Aperian will attempt to redirect the law enforcement agency to request that Customer Personal Data directly from Customer. As part of this effort, Aperian may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Aperian will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Aperian is legally prohibited from doing so.

- **General cooperation.** Each Party will reasonably cooperate with the other in any activities contemplated by this DPA and to enable each Party to comply with its respective obligations under Data Protection Law.

10. Jurisdiction-specific Terms

- **California (CCPA).** To the extent that Customer Personal Data is subject to the CCPA, Aperian agrees that it shall process Customer Personal Data as a service provider and shall not (a) retain, use or disclose Customer Personal Data for any purpose other than the purposes set out in the Agreement (including this DPA) and as permitted by the CCPA; or (b) "sell" personal information (as defined and interpreted within the requirements of the CCPA). The Parties agree that Customer's transfer of Customer Personal Data to Aperian is not a sale, and Customer provides no monetary or other valuable consideration to Aperian in exchange for the Customer Personal Data.
- **Europe**
  - **Processing Instructions.** Without prejudice to Section 3.3 (Customer Responsibilities), Aperian shall notify Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any processing instructions from Customer violate European Data Protection Laws.
  - **Sub-processor Obligations.** Aperian shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as required by this DPA (to the extent applicable, considering the nature of the services provided by the Sub-processor).
  - **Changes to Sub-processors.** Aperian will provide ten (10) days' prior notice via updating the Sub-processor List (or such other notification mechanism made available by Aperian) if it intends to make any changes to its Sub-processors. Customer may object in writing to Aperian's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g., if making Customer Personal Data available to the Sub-processor would violate European Data Protection Laws or weaken the protections for Customer Personal Data) by

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

notifying Aperian in writing to privacy@aperian.com within five (5) days of receiving notification from Aperian. In such event, the Parties shall discuss Customer's concerns in good faith with a view to achieving a mutually acceptable resolution. If the Parties cannot reach a mutually acceptable resolution, Aperian shall, at its sole discretion, either not appoint the Sub-processor, or permit Customer to suspend or terminate the affected Services in accordance with the Agreement without liability to either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

- **Application of the Standard Contractual Clauses.** The Parties agree that when the transfer of Customer Personal Data from Customer (as "data exporter") to Aperian Global (as "data importer") is a Restricted Transfer and European Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the SCCs, which shall be deemed incorporated into and form a part of this DPA, as follows:
  - Transfers from the EEA. In relation to transfers of Customer Personal Data protected by the EU GDPR, the SCCs shall apply, completed as follows:
    - Module Two (Controller to Processor) will apply;
    - in Clause 7, the optional docking clause will apply;
    - in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 10.2.3 of this DPA;
    - in Clause 11, the optional language will not apply;
    - in Clause 17, Option 1 will apply, and the SCCs will be governed by the EU Member State in which the Customer is established and if no such law Danish law;
    - in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the Customer is established and otherwise Denmark;
    - Annex I of the SCCs shall be deemed completed with the information set out in Annex A to this DPA; and
    - Subject to section 5.1 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in Annex B to this DPA;
  - Transfers from the UK. In relation to transfers of Customer Personal Data that are protected by UK Data Protection Laws, the SCCs: (i) shall apply as completed in accordance paragraph

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

(a)(i)-(viii) above; and (ii) shall be deemed amended as specified by the UK Addendum attached as **Annex D**, which shall deemed executed by the parties and incorporated into and form an integral part of this DPA. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

- Transfers from Switzerland. In relation to transfers of Customer Personal Data that is protected by the Swiss DPA, the SCCs will also apply in accordance with paragraph (a) above, with the following modifications:
  - references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;
  - references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;
  - references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law";
  - the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);
  - Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;
  - references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";
  - in Clause 17, the SCCs shall be governed by the laws of Switzerland; and
  - Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.
- It is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **Alternative transfer arrangements.** To the extent Aperian adopts an alternative lawful data export mechanism for the transfer of Customer Personal Data not described in this DPA (**"Alternative Transfer Mechanism"**), the Alternative Transfer Mechanism shall upon notice to Customer apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Customer Personal Data is transferred) and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism.
- **Privacy Shield.** Although Aperian does not rely on the Privacy Shield as a legal basis for transfers of Customer Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as Aperian is self-certified to the Privacy Shield it shall continue to process Customer Personal Data in compliance with the Privacy Shield Principles and agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the level of protection as is required by the Privacy Shield Principles.
- **Data Protection Impact Assessments.** To the extent Aperian is required under applicable European Data Protection Laws, Aperian shall provide reasonably requested information regarding Aperian's processing of Customer Personal Data under the Agreement to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

11. Limitation of Liability

- Any claim or remedy Customer or its Permitted Affiliates may have against Aperian, its employees, agents and Sub-processors, arising under or in connection with this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in the Agreement. Accordingly, any reference in the Agreement to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under and in connection with the Agreement and this DPA together.
- Aperian and its Affiliates' total liability for all claims from Customer and all Permitted Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all data processing agreements established under this DPA or the Agreement, including by Customer and all Permitted Affiliates, and shall not be

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

understood to apply individually and severally to Customer and/or to any Permitted Affiliate that is a contractual party to any such DPA.

- Aperian shall have no liability whatsoever in connection with any Sensitive Data ingested into the Services by Customer contrary to the provisions in the Agreement and this DPA.

12. Permitted Affiliates

- When a Permitted Affiliate becomes a party to the DPA, then such Permitted Affiliate shall be entitled to exercise its rights and remedies available under this DPA to the extent required under Data Protection Laws. However, if Data Protection Laws requires the Permitted Affiliate to directly exercise a right or remedy against Aperian directly by itself, the parties agree that to the extent permitted under law: (i) only the Customer that is the contracting entity to the Agreement shall exercise any such right or seek any such remedy on behalf of the Permitted Affiliate; and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Permitted Affiliates together, instead of doing so separately for each Permitted Affiliate. The Customer that is the contracting entity is responsible for coordinating all communication with Aperian under the DPA and be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

13. General

- The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Customer Personal Data is deleted from Aperian's systems.
- This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.
- Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement and this DPA, this DPA shall control with respect to any terms as they relate to Aperian's processing of any Customer Personal Data. Each Party acknowledges that the other Party may disclose the SCCs, this DPA and any privacy related provisions in the Agreement to any regulator, including European or US regulators, upon request.
- Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3.2, Aperian Global may periodically make modification to this DPA as may be required to comply with Data Protection Laws.
- The provisions of this DPA are severable. If any phrase, clause or provision or Annex (including the SCCs) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

provision, and the rest of this DPA or the remainder of the Agreement, which shall remain in full force and effect.

aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **Annex A**

Description of Data Processing / Transfer

Annex 1(A): List of parties	
Data exporter	**Name of the data exporter:** The entity identified as the Customer in the Agreement to which this DPA is attached. **Address:** The address for the Customer associated with its Aperian account or otherwise specified in this DPA or the Agreement. **Contact person's name, position and contact details:** The contact details associated with Customer's account, or otherwise specified in this DPA or the Agreement. **Activities relevant to the data transferred:** The activities specified in Annex 1(B) below. **Role (Controller/Processor):** Controller. **Signature and date:** See front end of this DPA.
Data importer	**Name of the data importer:** Aperian Global, Inc. ("Aperian") **Address:** 414 Fayetteville Street, 4th Floor, Raleigh, NC 27601, USA **Contact person's name, position and contact details:** privacy@aperian.com **Activities relevant to the data transferred:** The activities specified in Annex 1(B) below. **Role (Controller/Processor):** Processor. **Signature and date:** See front end of this DPA.

aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Annex 1(B): Description of the processing / transfer	
Categories of Data Subjects whose Personal Data is transferred	Current and former employees and other personnel of the Customer.
Categories of Personal Data transferred	The types of Customer Personal Data processed by Aperian are determined and controlled by the Customer in its sole discretion and may include, but is not limited to the following categories of Customer Personal Data: ● Account registration and management data (such as name, username, email address, password) ● Professional data (such as employer, employee ID number, business unit, performance) ● Device data (including IP address, browser/OS version, device configuration settings) ● User-generated content (such as responses to surveys, questions, comments and any user-generated content, including file attachments) ● Usage data (including feedback; information relating to the provision, use and performance of the Services; or any other information related to the data subject's utilization of the Services and offerings provided by Aperian).
Sensitive Data Transferred (if appropriate) and applied Restrictions or Safeguards:	The types of Customer Personal Data processed by Aperian are determined and controlled by the Customer in its sole discretion. Aperian does not intentionally collect any Sensitive Data in connection with the Services. Customer acknowledges that the Services are not designed to comply with data protection requirements that apply to Sensitive Data.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Customer Personal Data may be transferred on a continuous or one-off basis depending on the Customer's use of the Services and the Customer's processing instructions.
Subject matter of the processing:	The Customer Personal Data.
Nature of the Processing:	The provision of the Services as described in the Agreement and initiated by the Customer from time to time.
Purposes of the data transfer and further processing:	The Permitted Purposes (as defined in this DPA).
Period for which the Personal Data will be retained, or if that is not possible the criteria used to determinate that period, if applicable:	At the later of (i) the termination of the Agreement or, (ii) when all Customer Personal Data is deleted from Aperian's systems, in accordance with Section 13.1 of the DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	In line with the information provided above.

aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Annex 1(C): Competent supervisory authority	
Competent supervisory authority	The data exporter's competent supervisory authority will be determined in accordance with the European Data Protection Laws.

aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **Annex B**

  Security Measures

  Description of the technical and organisational measures implemented by Aperian (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

SECURITY MEASURES	MEASURES
Measures of pseudonymization of Personal Data and encryption data	**Pseudonymization** All user data is pseudonymized as a result of our normalized database structures. Profile, assessment, usage and other data tables only contain arbitrary user IDs.
	Encryption ● HTTPS encryption for data in transit (using TLS 1.2 or greater) on every login interface, using industry standard algorithms and certificates. ● Data at rest is encrypted using the industry standard AES-256 algorithm.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Confidentiality** We take the following measures to ensure Confidentiality of our Aperian learning platform and related webtools: ● Ensure that any person authorized to process the data is subject to an obligation of confidentiality ● Secure transmission of credentials using TLS 1.2 (or greater) ● Systems used in the provision of the Services are configured to authenticate personnel with a unique user ID and password ● Network segmentation ● Passwords require a defined minimum complexity ● We take these additional measures for our internal product development and IT processes: ● Use of Multi-Factor Authentication (MFA) for systems processing sensitive data. ● Differentiated rights system based on security groups and access control lists ● Passwords must be changed at regular intervals • Process to deactivate accounts of personnel upon termination or job change ● Guidelines provided to users for handling of passwords ● Access controls to infrastructure that is hosted by cloud service provider ● Access right management including authorization concept, implementation of access restrictions, implementation of the “need-to-know” principle, managing of individual access rights. ● Annual security and privacy awareness training and confidentiality agreements for personnel and external staff ● Segregation of responsibilities and duties ● Comprehensive employee screening/background checks

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

	• Secure development lifecycle process followed in software development
	Integrity We take the following measures to ensure Integrity of our GlobeSmart platform and related webtools: • Secure network interconnections ensured by firewalls, including perimeter firewalls, etc. • Logging authentication and monitored logical system access • We take these additional measures for our internal product development and IT processes: • Protocol of the use of administration tools • Protocol of system generation and modification of system parameters • Complete protocol of all instances • Anti-malware protections • Logging of transmissions of data from IT systems that stores or processes data
	Availability and resilience • Full redundancy of network and deployments in multiple availability zones • Data is backed up to encrypted data stores • Protection of stored backup media

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Use of electronic data processing devices

We take the following measures to limit access of unauthorized persons to systems where data is used or processed with electronic data processing devices:

- Regulations and instructions for access control, including role-based access permissions
- Process to adjust permissions upon role changes
- Assignment of rights for data-input as well as for information, modification and deletion of stored data
- Regulated procedure for granting, changing and revocation of access rights
- Selective access for files and functions
- Automatic screensaver protection in case of inactivity
- Requirement of user identifiers (Passwords) for files, system data, application data
- Logging access to specific data (e.g.: Console log, machine Log)
- Password policy at the level of configuration of IT-systems
- Documented access requests and management authorization for access to production environment
- Administrative access privileges restricted to authorized personnel

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Measures for ensuring the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident	• Documented Continuity Planning and Disaster Recovery Plans that are reviewed periodically with annual standard maintenance and assessment • Disaster recovery processes to restore data and processes • Recovery Time Objective (RTO) • Recovery Point Objective (RPO) • Capacity management measures to monitor resource consumption of systems as well as planning of future resource requirements. • Procedures and documented response plan for handling and reporting incidents (incident management, mitigation and remediation) including the detection and reaction to possible security incidents • Production data is backed up daily and at least weekly as a full backup. All backups are encrypted form (AES-256 standard).
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	• Process to continually review and improve the suitability, adequacy and effectiveness of security measures • Internal and external audits • Security checks (e.g. penetration tests) conducted by external parties • ISO 27001 audits • With respect to code, annual penetration tests and quarterly vulnerability assessments on production infrastructure and remediation efforts prioritized and applied against critical and high-risk issues • Remediation plans are developed and implemented when findings are identified

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Measures for user identification and authorization	• Secure network interconnections ensured by MFA, firewalls etc. • Logging authentication and monitored system access • Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept in accordance to the "need-to-know" principle • Web Application Firewall (WAF)
Measures for the protection of data during transmission	We take the following measures to ensure Integrity of our GlobeSmart platform: All server connections are over HTTPS/TLS (SHA256withRSA). Our web site receives an A+ security rating from SSLLabs, which you can view here: https://www.ssllabs.com/ssltest/analyze.html?d=globesmart.aperianglobal.com
Measures for the protection of data during storage	Aperian learning platform databases and backups are encrypted via RDS/AES-256 encryption.

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Measures for ensuring physical security of locations at which data are processed	**Entry controls** Most of our employees work remotely and are subject to our Secure Areas policies. The Aperian learning platform is hosted on state-of-the-art, high-security data centers located in the USA as follows: Aperian learning portal (https://aperian.com) on Amazon Web Services (AWS) These cloud providers security information can be viewed here: https://aws.amazon.com/compliance/ See our complete Subprocessor List for more details. https://aperian.com/subprocessor-list

aperian

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **Annex C**

  Sub-processor List

  Hosting, content and analytics services

Name	Description	Address
Amazon Web Services, Inc.	Hosting services	410 Terry Avenue North Seattle, WA 98109-5210, USA
Google, LLC	Hosting services	Google Cloud Platform (GCP), 1600 Amphitheatre Parkway, Mountain View, California 94043, USA
Databox, Inc.	User behavior analytics	6 Liberty Square PMB 471 Boston, MA 02109, USA Registration: 001118210
Mixpanel, Inc.	User behavior analytics	One Front Street, 28th Floor San Francisco, CA 94111, USA

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Rustici Software LLC	Content asset management	210 Gothic Court #100 Franklin, TN 37067, USA

Email and messaging delivery services

Name	Description	Address
Appcues, Inc.	Onboarding and product tour system	177 Huntington Ave Ste 1703, PMB 94414, Boston, MA 02115, USA
Braze, Inc.	Onboarding and email system	330 W 34th St 18th floor New York, NY 10001, USA Registration #: 4103543
SendGrid, Inc.	Email invitations	1801 California Street, Suite 500 Denver, Colorado 80202, USA

Application integrations

Name	Description	Address
Alchemer LLC	Customer experience and survey builder	168 Centennial Parkway Unit #250, Louisville, CO 80027, USA

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Auth0, Inc.	Identity management and authentication	10900 NE 8th Street Suite 700, Bellevue, WA 98004, USA
Stripe, Inc.	Customer subscription management	510 Townsend Street, San Francisco, CA 94103, USA
Typeform, S.L.	Forms	Carrer Bac de Roda, 163, 08018 Barcelona, Spain
Zapier, Inc.	Service that moves quiz completion data to analytics platform	243 Buena Vista Ave #508, Sunnyvale, CA 94086, USA

Customer success and technical support services

Name	Description	Address
Clientsuccess, Inc.	Customer success platform	770 E. Main St. #151 Lehi UT 84043, USA Registration #:8610552-0143
Zendesk, Inc.	Help desk and ticketing software	1019 Market Street, San Francisco, CA 94103, USA

Platform maintenance and support

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

Name	Description	Address
Moodle Pty Ltd (Moodle US)	Platform maintenance and support	8101 College Blvd, Suite 100 Overland Park, Kansas 66210, USA
Sparkbox, Inc	Platform maintenance and support	123 Webster Street, Studio 2 Dayton, OH 45402, USA
Verve Systems Pvt. Ltd.	Platform maintenance and support	904, 9th Floor, Venus Atlantis, 100 Feet Road, Satellite, Prahlad Nagar, Ahmedabad, 380015 India

Besides Aperian Global, Inc., Non-EU Affiliates which may process Customer Personal Data in order to deliver the Services and provide support include:

- Aperian (India) Management Consulting Private Ltd – Subsidiary of US, #150/1, Ground Floor, Infantry Road, Bengaluru – 560001, Karnataka, India

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

- **Annex D**

  UK Addendum

  This Annex D forms part of this DPA and applies in accordance with Section 10.2.4(b) (Transfers from the UK) of the DPA.

Start Date	The date of the Agreement.	
Parties	Exporter	Importer
Parties' details	**Name:** The entity identified as the Customer in this DPA. **Address:** The address for the Customer associated with its Aperian account or otherwise specified in this DPA or the Agreement. **Contact person's name, position and contact details:** The contact details associated with Customer's account, or otherwise specified in	**Name:** Aperian Global, Inc. ("Aperian") **Address:** 414 Fayetteville Street, 4th Floor, Raleigh, NC 27601, USA **Contact person's name, position and contact details:** Data protection enquiries can be addressed to privacy@aperian.com

414 Fayetteville St.
4th Floor
Raleigh, NC 27601
United States
Phone: +1 984 247 1344

	this DPA or the Agreement.	

Addendum SCCs	The Approved SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the approved SCCs brought into effect for the purposes of this Addendum: See Section 10.2.4(b) of the DPA.

Appendix Information	See Annex A

Ending this Addendum when the Approved Addendum changes	Neither Party

Mandatory Clauses	Part 2: Mandatory Clauses of the UK Addendum, as it is revised under Section 18 of those Mandatory Clauses.