DPA 2023v1

Data Processing Addendum

1. Roles and Responsibilities

1.1. **Roles.** Showpad shall be considered Processor or Service Provider (or similar applicable definition), and the Customer shall be considered Controller or Business (or similar applicable definition), under Applicable Data Protection Law with regard to Showpad's Processing of Customer Personal Data in the framework of this Data Processing Addendum (the "DPA").

1.2. **Instructions.** The Customer instructs Showpad to Process Customer Personal Data as necessary for Showpad to provide the Products and Services to the Customer in accordance with the Agreement, including this DPA, and/or as separately instructed by the Customer. Showpad shall inform the Customer if, in Showpad's opinion, an instruction of the Customer, or the Customer's representatives, Administrators, or Authorized Users infringes an Applicable Data Protection Law. Where there is a legal requirement under Applicable Data Protection Law for Showpad to Process Customer Personal Data outside of the instructions of the Customer or the Customer's representatives, Administrators, or Authorized Users, Showpad shall inform the Customer of that legal requirement before Processing, unless prohibited by Applicable Data Protection Law.

1.3. **Showpad Responsibilities.**

1.3.1. When Processing Customer Personal Data, Showpad shall: (i) not Process the Customer Personal Data outside of the relationship between Showpad and the Customer unless the Customer has provided consent or another mandatory legal requirement under Applicable Data Protection Law applies; (ii) not Process Customer Personal Data with Personal Data Showpad receives from, or on behalf of, other customers, or collects from Showpad's interaction with the Customer, unless otherwise permitted by Applicable Data Protection Law; (iii) ensure that access to Customer Personal Data occurs on a "need-to-know" basis and "as required"; (iv) ensure implementation of confidentiality provisions, or statutory obligations of confidentiality on persons authorised to process Customer Personal Data; (v) not Sell or Share Customer Personal Data; and (vi) adhere to the security provisions as set forth in Annex 2.

1.3.2. Showpad shall comply with Applicable Data Protection Law and notify the Customer if Showpad can no longer meet Showpad's obligations under Applicable Data Protection Law. If Showpad can no longer meet Showpad's obligations under Applicable Data Protection Law, then the Customer may, upon notice, take reasonable and appropriate steps to remediate unauthorized uses of Customer Personal Data, consistent with and in accordance with Applicable Data Protection Law, by requesting reasonable documentation from Showpad that verifies Showpad's compliance with its obligations under Applicable Data Protection Law.

2. Sub-Processors

2.1. **List of Sub-Processors.** A list of the then current Sub-Processors of Showpad, including the specifics of their Processing activities, is available through the administrator section of the Products and Services (admin settings > privacy > data agreement specifics), via the Showpad public website (www.showpad.com/subprocessors), or upon request.

2.2. **Addition or Replacement.** Showpad shall publish any additions and/or replacements with respect to its Sub-Processors on the Showpad public website at least thirty (30) days in advance. The Customer may subscribe to that webpage to receive notifications with respect to additions and/or replacements of the Sub-Processors. Any publication under this Section 2.2 shall be considered a notification to the Customer. Each publication will be confirmed in an email notification sent by Showpad to the addresses as subscribed.

2.3. **Objection.** The Customer shall be allowed to object to an addition or replacement of Sub-Processors under Section 2.2 above by providing an opposition thereto, which opposition shall be based upon reasonable and substantial grounds. The Customer must provide Showpad with notice of any such opposition within twenty (20) days following the relevant notification by Showpad under Section 2.2, in the absence of which the Customer shall have accepted the respective addition or replacement Sub-Processor(s).

2.4. **Resolution.** Following a timely opposition under Section 2.3 above, Showpad shall have the right to resolve the Customer's opposition through one of the following solutions (to be selected at Showpad's sole discretion). Showpad may: (i) cancel its plans to use the relevant Sub-Processor or offer an alternative; (ii) take the corrective steps as reasonably requested by the Customer in its opposition in order to remove the reasons for the Customer's opposition and proceed with the respective Sub-Processor; or (iii) cease to provide, temporarily or permanently, the particular component of the Products and Services that is impacted by such addition or replacement, subject to the mutual agreement of the Parties to adjust the applicable fees for the applicable Products and Services under the Agreement.

2.5. **Sub-Processor Obligations.** Showpad has executed a written contract with each Sub-Processor that meets the respective data protection obligations of this DPA and provides sufficient guarantees to implement

appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of this DPA. When a Sub-Processor is certified under a Third-Party Assurance Report (TPAR) that relates to the Processing activities covered under this DPA, the Parties agree that such certification satisfies the applicable requirements of this DPA to the extent such TPAR i) was issued within the prior twelve (12) months, and ii) confirms there are no known material deficiencies in the controls audited under such TPAR.

2.6. **Responsibilities**. In the event a Sub-Processor fails to fulfill its data protection obligations, Showpad shall remain liable to the Customer for the performance of that Sub-Processor's obligations.

3. International Data Transfers

3.1. **Transfer of Personal Data into or Circulation Within EEA.** Where Showpad transfers Customer Personal Data into the EEA and/or circulates Customer Personal Data to a Sub-Processor within the EEA, the provisions of GDPR shall apply and will regulate such transfer or circulation. The Customer agrees that transfer into the EEA and/or circulation within the EEA under the provisions of GDPR are adequate and provide for appropriate safeguards to allow for such transfers to take place.

3.2. **International Transfer of Personal Data.** Showpad shall ensure where Customer Personal Data is transferred internationally from the EEA to an onward Sub-Processor outside of the EEA, such transfer shall, to the extent required by Applicable Data Protection Law, be covered under:

3.2.1. a so-called "adequacy decision" (e.g., in execution of article 45 of the GDPR, including Canada adequacy decision and Japan adequacy decision);

3.2.2. a so-called "appropriate safeguard" (e.g., in execution of article 46 of the GDPR, including binding corporate rules, applicable EU standard contractual clauses, or an approved code of conduct); and/or

3.2.3. such other method as allowed per Applicable Data Protection Law.

If for any reason an applicable data transfer mechanism is deemed inadequate by the appropriate regulatory body, the Parties will act in good faith and, where necessary, establish the appropriate data transfer mechanism(s) to provide for such international transfer.

3.3. **EU Model Clauses.** Where Showpad, Inc. is the contracting party to this DPA, and to the extent Showpad, Inc., is importing Personal Data into the US originating from the EEA, UK, or Switzerland, Showpad, Inc., shall abide by and accept the provisions further detailed in Annex 3.

4. Assistance

4.1. **Tools And Features of the Products and Services.** During the term of the Agreement, the Customer can use the functionalities of the user interface of the Products and Services to access, retrieve, download, correct, and/or delete Customer Content and/or individual records of a Data Subject. Retrieval and download of Customer Content shall occur in its native format. Retrieval and download of analytics relating to the use of the Products and Services shall occur by making such analytics available to the Customer in a structured, commonly used and machine-readable format (e.g., .csv format).

4.2. **Showpad Assistance.** To the extent that the functionalities under Section 4.1 above are not sufficient to permit the Customer to fulfill the Customer's obligations under Applicable Data Protection Law, Showpad shall cooperate with the Customer's reasonable requests for assistance in fulfilling such obligations.

4.3. **Data Subjects Requests.** Showpad shall not act upon direct requests or instructions from Data Subjects regarding Customer Personal Data, nor shall Showpad provide any information to Data Subjects, unless and to the extent the Customer specifically instructs Showpad to do so. Showpad shall forward such Data Subject requests to the appropriate customer without undue delay after Showpad determines the identity of the respective customer. The foregoing shall not prohibit Showpad from communicating with a Data Subject in order to determine the Showpad customer to which the respective requests relate.

4.4. **Direct Requests from Supervisory Authorities or Law Enforcement.** Showpad shall as soon as practicable notify the Customer about any legally binding request for disclosure of the Customer Personal Data by a supervisory authority or law enforcement authority (including without limitation any foreign administrative or judicial authority) unless otherwise prohibited by law from doing so. Unless Showpad's cooperation is required by law, Showpad shall cooperate with such supervisory authority or law enforcement authority only and to the extent instructed by the Customer. Where Showpad is obliged to cooperate with such supervisory authority or law enforcement authority outside of the Customer's instruction, Showpad shall limit the disclosure of the Customer Personal Data to what is necessary to meet the legal obligation.

4.5. **Data Protection Impact Assessment ("DPIA") / Third Party Assurance Report (TPAR) / Certifications / Documentation.** At the Customer's reasonable request, Showpad shall provide the Customer with documentation, a TPAR, and/or evidence of certifications necessary to assist the Customer in carrying out a DPIA, to demonstrate Showpad's compliance with this DPA and/or Applicable Data Protection Law, and to enable the Customer to demonstrate compliance with the Customer's obligations. Any documentation, TPAR, and/or certification shared by Showpad shall be considered Confidential Information of Showpad and shall be covered under applicable confidentiality provisions in the Agreement or in an applicable non-disclosure agreement.

5. Personal Data Breach

5.1. **Notification.** Showpad shall notify the Customer without undue delay, and within no more than forty-eight (48) hours, after becoming aware of a Personal Data Breach. Such notification shall at least:

5.1.1. describe the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

5.1.2. contain the name and contact details of the data protection officer or other contact point of Showpad where more information can be obtained;

5.1.3. describe the likely consequences of the Personal Data Breach; and

5.1.4. describe the measures taken or proposed to be taken by Showpad to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.2. **Documentation.** Showpad shall document Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects, and the remedial action taken, and provide, on request, such documentation to the Customer that the Customer requires for the supervisory authority to verify compliance.

6. Audits

6.1. **Customer Audit.**

6.1.1. If the Customer requests information and/or an audit for which the scope of the request is addressed in a TPAR issued within the prior twelve (12) months confirming there are no known material deficiencies in the controls audited under such TPAR, the Customer agrees to accept the findings presented therein in lieu of requesting additional information or an audit of the same controls already covered in such TPAR.

6.1.2. Where i) the scope of the applicable TPAR does not address the controls necessary to demonstrate Showpad's compliance with this DPA and/or Applicable Data Protection Law, ii) the applicable TPAR shows material deficiencies in the controls audited under such TPAR, or iii) a Personal Data Breach occurs, Showpad agrees that the Customer may conduct an on-site audit under the terms of this Section 6 at Showpad's premises used for the exploitation of the Products and Services in order to verify compliance with this DPA and/or the Applicable Data Protection Law for such matters not adequately addressed or found to be material deficiencies under the TPAR.

6.1.3. Requests for audit shall be addressed to the Showpad data protection officer (privacy@showpad.com), and shall include: (i) the requested audit scope; and (ii) the systems, processes, procedures, and documents to be audited.

6.1.4. Unless and to the extent Section 6.2 applies, audits under this Section 6.1 may only be conducted:

6.1.4.1. upon prior written notice of at least thirty (30) days, upon such date as mutually agreed upon by the Parties in good faith (which approval shall not be unreasonably withheld or delayed);

6.1.4.2. by auditors who have agreed to, or to whom apply, confidentiality undertakings at least similar to the confidentiality undertakings as applicable between the Customer and Showpad;

6.1.4.3. by auditors that abide by regulations applicable to the Showpad premises, including access control regulations and site safety regulations;

6.1.4.4. not more than once per year, unless otherwise required by Applicable Data Protection Law;

6.1.4.5. during normal business hours of Showpad and without significant interruption of Showpad's business; and

6.1.4.6. under a "read only" access to the systems, information, and documents being the subject matter of the audit.

6.2. **Regulatory Audit.** If the Customer is required under Applicable Data Protection Law by a supervisory authority to perform an on-site audit at Showpad's premises on Showpad's systems and procedures related to or used for the Products and Services, the Customer shall provide reasonable prior notice to Showpad. Such regulatory audit shall be executed, if and to the extent legally allowed by Applicable Data Protection Law, in accordance with the provisions of this Section 6, or, if full compliance with Section 6 is not possible, as close to the provisions of this Section 6 as reasonably possible.

6.3. **Action Plan.** In the event an audit under this Section 6 reveals material non-conformities with this DPA or Applicable Data Protection Law, Showpad will, at its cost: (i) promptly deliver to the Customer an action plan to mitigate such non-conformities without delay; and (ii) perform the necessary mitigation actions as soon as reasonably possible.

6.4. **Cost.** Each Party will bear its own costs in relation to the audit. Notwithstanding the foregoing, where the Customer audit plan (or aspects thereof) is unreasonable and/or materially exceeds what is customary in the applicable industry for the types of Products and Services offered by Showpad, the Parties shall meet in good faith to either adjust the audit plan to address removal of the non-standard requests or determine an equitable division of costs for the non-standard requests. In case the results of the audit reveal a material non-conformity regarding this DPA and/or Applicable Data Protection Law, Showpad shall, upon request, reimburse the Customer for such audit costs as reasonably incurred by the Customer in relation to the material non-conformity in question.

7. Term

This DPA will terminate simultaneously and automatically with the termination or expiration of the Agreement.

8. Definitions

8.1. Capitalized terms not otherwise defined herein have the meanings given to them in the Agreement. The terms "**Business**," "**Service Provider**," and "**Share**" shall have the meanings given in the CCPA.

8.2. "**Administrator(s)**" means the individual(s) employed or engaged by the Customer having an "administrator," "account owner," or similar role with regard to the Products and Services, and who is or are responsible within the Customer organisation for maintaining, supporting, testing, or administering all or part of the Products and Services or Authorized User accounts.

8.3. "**Applicable Data Protection Law**" means applicable data protection laws, including, but not limited to, (a) the GDPR; (b) the UK Data Protection Act 2018; (c) the Swiss federal data protection act; (d) the CCPA; (e) the VCDPA; (f) the CPA; (g) the UCPA; and (h) the CTDPA.

8.4. "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.

8.5. "**CPA**" means the Colorado Privacy Act.

8.6. "**CTDPA**" means the Connecticut Data Privacy Act.

8.7. **"Customer Personal Data"** means Personal Data that is part of i) the Customer Content or ii) the analytics relating to the use of the Products and Services.

8.8. "**EEA**" or "**European Economic Area**" means the territory of the EU Member states as well as EFTA Member States.

8.9. **"EU Model Clauses"** means such clauses as approved by the EU Commission in its Commission implementing decision (2021/914/EU) 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.

8.10. "**GDPR**" means the General Data Protection Regulation (EU/2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

8.11. "**Personal Data Breach**" means a 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 Showpad.

8.12. "**Processing**", "Process" or "Processed" means any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, retention, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

8.13. "**Processor**" means the entity (a Service Provider) that Processes Personal Data on behalf of, and under instruction of, a Controller.

8.14. "**Prospect**" means a third party with whom the Customer's Administrators and/or Authorized Users are interacting through the Showpad Products and Services by sharing certain Customer Content, or with whom that third party in question is re-sharing Customer Content through the Showpad Products and Services.

8.15. "**Sell**" or "**Sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary or other valuable consideration, or for a third party's commercial purpose.

8.16. "**Sub-Processor**" means any party, other than Showpad or the Customer, carrying out specific Processing activities on Customer Personal Data for Showpad in relation to the Products and Services.

8.17. **"Third Party Assurance Report"** or **"TPAR"** means an applicable SOC, ISO, ISAE or similar audit report or certification issued by a qualified third-party auditor (e.g., ISO 27001, ISO 27701, ISAE 3402, SSAE 16 SOC 2, and/or equivalent) as well as the bridge letter related thereto.

8.18. "**UCPA**" means the Utah Consumer Privacy Act.

8.19. "**VCDPA**" means the Virginia Consumer Data Protection Act.

Annex 1. Specification of the Products and Services

1. Purpose / Description of the Products and Services Provided by Showpad

Processing of Personal Data relating to the Showpad sales enablement solution provided under a "Software as a Service" model, consisting of i) an online web-based back-end that stores, analyzes, manages, distributes, and Processes Personal Data and Customer Content, as well as ii) interacting front-end clients (e.g., the Showpad mobile application) and/or web interfaces (e.g., webapp, plugins), that enable sales and marketing teams to create and manage interactions between Administrators, Users, and Prospects in a data-driven way.

2. Categories of Data Subjects Whose Personal Information Is Being Processed by the Products and Services

Showpad Content: Authorized Users / Administrators / Prospects / re-shared Prospects

Showpad Coach: Authorized Users / Administrators

3. Categories of Personal Data Processed

Depending on the role within the Products and Services (Administrator, User, or Prospect) certain categories of Personal Data may be processed as follows:

- Contact information (e.g., name, email address, telephone number)
- Account information (e.g., password, profile picture, role, device information, logon information)
- Connection information (e.g., IP address, city)
- Customer Content (e.g., documents, presentations, audio files, video files, and trainings uploaded onto the Products and Services by the Customer or as created by the Customer on the Products and Services)
- Usage and Behavior Statistics (e.g., sessions, in app views, shares, channel subscriptions, number of interactions with the Customer Content, and training results)
- Communications within the Products and Services (e.g., Chat content, reviews, comments, Administrator announcements)
- Information from third party integrations (e.g., connected calendars, CRM data, and marketing data)

More information can be obtained from the privacy settings of the Products and Services (admin settings > privacy > data agreement specifics) or on request.

The Products and Services do not process Sensitive Personal Data and are not intended for processing Sensitive Personal Data.

4. Processing Operations

Personal Data as covered under this DPA may be subject to the following processing activities:

- Storage and other processing operations necessary to
  a. provide, maintain, and/or support the Products and Services
  b. provide the Customer with the analytics generated by the Products and Services resulting from interactions with Customer Content;
- Consultation of Personal Data by Authorized Users and Administrators through the Products and Services' user interface; and/or
- Disclosures in accordance with this DPA or the Agreement or as compelled by applicable laws.

5. Duration of Processing by the Products and Services

Processing will run for as long as the respective Personal Data resides on the Showpad Platform (in the production and back-up environments).

Unless otherwise agreed or reasonably requested by the Customer, the Personal Data is retained and backed-up within the Products and Services for up to 200 calendar days after expiration or termination of the DPA ("Back-up Term") through Showpad's standard back-up schedules for the Products and Services, after which the Personal Data shall be irrevocably and permanently deleted.

Showpad shall not Process the Personal Data during the Back-up Term for any other purpose than to ensure back-up availability.

6. Sub-processors

Current and future Sub-Processors of Showpad, as well as the respective Processing activities shall be as published on www.showpad.com/subprocessors

7. Frequency of Transfers

The transfers of Customer Personal Data will be continuous.

Annex 2. Security

A. General. When providing the Products and Services, Showpad shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures (in particular based upon the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed) to ensure a level of security appropriate to the risk, including, *inter alia,* as appropriate:

a) the pseudonymization and encryption of Personal Data;
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 Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

B. Information Security Management System ("ISMS"). Showpad has developed and implemented a security assurance program using global privacy and data protection best practices. This ISMS:

a) is audited on a regular basis by an external independent audit firm having the competent capabilities; and
b) shall be maintained and remain in place in line with the provisions of the ISO/IEC 27001:2013, ISO/IEC 27701:2019, and ISAE 3402 standards (or equivalent standards) for the duration of this DPA.

C. Security Measures. Showpad has developed and implemented specific security measures, including:

1. **Physical access control.** Technical and organizational measures to prevent unauthorised persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers, and related hardware), where Personal Data is Processed, include:
   - establishing security areas, restriction of access paths;
   - establishing access authorizations for employees and third parties;
   - access control system (ID reader, magnetic card, chip card);
   - key management, card-keys procedures;
   - door locking (electric door openers, etc.);
   - surveillance facilities, video/CCTV monitor, alarm system; and
   - securing decentralized data processing equipment and personal computers.

2. **Virtual access control.** Technical and organizational measures to prevent data processing systems from being used by unauthorised persons include:
   - user identification and authentication procedures;
   - ID and password security procedures (special characters, minimum length, change of password);
   - automatic blocking (e.g., password or timeout);
   - monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous password attempts;
   - creation of one master record per user, user master data procedures, per data processing environment; and
   - encryption of archived data media.

3. **Data access control.** Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified, or deleted without authorization, include:
   - internal policies and procedures, including with regard to data minimisation and "need to know access";
   - control authorization schemes;
   - differentiated access rights (profiles, roles, transactions, and objects);
   - monitoring and logging of accesses;
   - disciplinary action against employees who access Personal Data without authorization;
   - reports of access;
   - access procedure;
   - change procedure;
   - deletion procedure; and
   - encryption.

4. **Disclosure control.** Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on storage media (manual or electronic), and that Showpad can verify the companies or other legal entities to which Personal Data is disclosed, include:
   - encryption/tunneling;
   - logging; and
   - transport security.

5. **Entry control.** Technical and organizational measures to monitor whether data has been entered, changed, or removed (deleted) from data processing systems, and by whom, include:
   - logging and reporting systems;
   - audit trails and documentation.

6. **Control of instructions.** Technical and organizational measures to ensure that Personal Data is processed solely in accordance with the instructions of the Controller include:
   - unambiguous wording of the contract;
   - formal commissioning (request form); and
   - criteria for selecting Processors.

7. **Availability control.** Technical and organizational measures to ensure that Personal Data is protected against accidental destruction or loss (physical or logical) include:
   - backup procedures;
   - mirroring of hard disks (e.g., RAID technology);
   - uninterruptible power supply (UPS);
   - remote storage;
   - anti-virus and firewall systems; and
   - disaster recovery plan.

8. **Separation control.** Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:
   - separation of databases;
   - “internal client” concept / limitation of use;
   - segregation of functions (production/testing); and
   - procedures for storage, amendment, deletion, and transmission of data for different purposes.

Annex 3. EU Model Clauses - EU Controller to Non-EU or EEA Processor (*)

In the case and to the extent Showpad, Inc., is the contracting party to this DPA, and to the extent Showpad, Inc., is importing Personal Data into the United States originating from the EEA, UK, or Switzerland, Showpad, Inc., accepts the provisions of the EU Model Clauses, which, as acknowledged by Showpad, Inc., are incorporated herein by reference as detailed below:

1. Under the EU Model Clauses, parties shall respectively be deemed "Data Exporter" and "Data Importer" as follows:

- **Data Exporter:**	
Identification	The Customer as identified in the Agreement
Role	Controller

- **Data Importer:**	
Name	Showpad, Inc.
Address	1 N State Street, 11th Floor, Chicago, IL 60602 USA
Contact Person	Data Protection Officer / privacy@showpad.com
Relevant activities	As specified in Annex 1 to this DPA
Role	Processor

2. As a consequence of the roles identified in No. 1. above, the provisions of **"Module Two"** of the EU Model Clauses (international data transfer from controller to processor) shall be applicable in the relationship between Showpad, Inc., and the Customer.

3. The security measures taken by Showpad, Inc., shall be as set forth in Annex 2 to the DPA.

4. The optional wording as set forth in Clauses 7 (docking) and 11 (redress) shall not apply.

5. In execution of Clause 9 of the EU Model Clauses, Sub-Processor authorisation shall occur under the principle of a "general authorisation" as further detailed in the DPA.

6. In execution of Clause 17 of the EU Model Clauses, the EU Model Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

7. In execution of Clause 18 of the EU Model Clauses, any dispute arising from these Clauses shall be resolved by the courts of Brussels, Belgium.

8. Annex 1 to the EU Model Clauses is completed as follows:
   A. List of Parties to these EU Model Clauses shall be as set forth in Section 1 of Annex 3 to this DPA;
   B. Description of transfers shall refer to Annex 1 to this DPA;
   C. The supervisory authority with responsibility for ensuring compliance by the data exporter shall be:
      - Where the data exporter is established:
        a. in the EEA: the supervisory authority where the data exporter is established
        b. in the UK: the information commissioner's office
        c. in Switzerland: Federal Data Protection and Information Commissioner
      - Where the data exporter is not established in the EEA, UK, or Switzerland but has appointed a representative in such territory, the supervisory authority where such representative is located;
      - Where the data exporter is not established in the EEA, UK, or Switzerland and has not appointed a representative in any such territory, the supervisory authority having authority over the Data Subjects whose personal data is being processed.
9. Annex 2 to the EU Model Clauses shall refer to Annex 2 to this DPA

10. Annex 3 to the EU Model Clauses shall not be applicable in light of the general authorization.

11. Signature of this DPA shall unequivocally serve as a binding acceptance of the EU Model Clauses.

12. **Transfers outside of the UK and Switzerland**. Where there is export of Customer Personal Data out of the UK and Switzerland:
   A. **For the UK:** the EU Model Clauses shall be interpreted in accordance with "UK Addendum to the EU Commission Standard Contractual Clauses" ("UK Addendum") as published by the UK Information Commissioner's Office. For the avoidance of doubt, the UK Addendum shall be deemed effective concurrently with EU Model Clauses.
   B. **For Switzerland:** the EU Model Clauses shall be interpreted in accordance with the statement of the Swiss Data Protection and Information Commissioner ("**FDIPC**") of 27 August 2021). The EU Model Clauses shall apply with the following adjustments:

- the FDPIC shall be the competent supervisory authority insofar as the data transfer is governed by the Swiss Federal Act on Data Protection ("FADP");
- the applicable law shall be the law of the EEA Member State as specified in above; and
- the courts of the EEA Member State as specified above shall have jurisdiction; however, the term "EEA Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of bringing a claim for their rights in their place of habitual residence in Switzerland.

For the avoidance of doubt, the Swiss interpretation shall be deemed effective concurrently with the EU Model Clauses.