DATA PROCESSING AGREEMENT
FOR PROCESSORS AND SUBPROCESSORS

This Data Processing Agreement ("**DPA**") shall govern any services provided to you and your Affiliates ("**Customer**") by INK Content, Inc. ("**INK**") as a Processor or Sub-processor (as defined below) (the "**Services**"). INK and Customer shall each be referred to herein as a "**Party**" and together as "**Parties.** This DPA supplements, is incorporated into, and will remain in effect for the term of any agreement between the Parties, including but not limited to any executed or click-through Terms of Service (the "**Agreement**"), the duration of Services, or the processing of Customer Data, whichever is later (the "**Term**"). This DPA is entered by INK and Customer on _____, 2024 ("**Effective Date**").

The Parties agree as follows:

1. Definitions

Capitalised terms used but not defined in this DPA shall have the same meanings as set out in the Agreement, if applicable. For the purposes of this DPA:

1.1 "Affiliate(s)" means any person or entity that controls, is controlled by, or is under common control with such entity, whether as of the date of the Agreement or thereafter. For purposes of this DPA, "**control**" means ownership or control, directly or indirectly, of more than 50% of the outstanding voting stock of an entity or otherwise possessing the power to direct the management and policies.

1.2 "**Applicable Privacy Laws**" means all applicable privacy and data protection laws and regulations anywhere in the world, including, where applicable, 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("**GDPR**"), the EU Directive 2002/58/EC on privacy and electronic communications (in all cases, as amended, superseded or replaced), and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and its implementing regulations ("**CCPA**").

1.3 "**Controller**" means the natural or legal person or entity who determines the purposes and means of the processing of Personal Data.

1.4 "**Data Breach**" means a breach of security leading to accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access of Customer Data.

1.5 "**Customer Personal Data**" means any and all Personal Data that is provided to INK or otherwise collected and/or accessed by INK on behalf of Customer and/or its affiliates in the course of providing the services under the Agreement.

1.6 "**New EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 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, completed as set forth in the Appendix to this DPA**.**

1.7 "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

1.8 "**Processor"** means an entity that processes Customer Personal Data on behalf of, and in accordance with the instructions of, a Controller.

1.9 "**Sub-processor**" means an entity engaged by a Processor who agrees to receive from the Processor Personal Data exclusively intended for the processing activities to be carried out as part of the Services.

1.10 "UK GDPR" means the UK General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.11 "UK SCC Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/), completed as set forth in this DPA.

2. Role of the Parties and Nature of the Personal Data

2.1 For purposes of this DPA, Customer may act as a Controller, or it may act as a Processor of one of its customers. INK therefore acknowledges that it may act as a Processor of Customer when Customer is acting as a Controller or a Sub-processor of Customer when Customer is acting as a Processor. Where Customer acts as a Processor, Customer is obligated contractually and / or under Applicable Privacy Laws to flow down certain data protection related obligations to its appointed Sub-processors. Therefore all obligations placed on Processors in this DPA shall apply to INK regardless of whether INK acts as a Processor or Sub-processor.

2.2. The Parties acknowledge and agree that INK will process Customer Personal Data as described in Appendix 1 (Data Processing Description) of this DPA.

3. INK's Compliance

3.1 INK warrants and undertakes to process Customer Personal Data only for the limited and specified purposes

set out in the Agreement and/or as otherwise lawfully instructed by Customer in writing (email or otherwise), except where otherwise required by applicable law. INK will immediately inform Customer if, in its opinion, an instruction is in breach of Applicable Privacy Laws. INK acknowledges and confirms that it does not receive any Customer Data as consideration for any services or other items that INK provides to Customer. INK shall not have, derive or exercise any rights or benefits regarding Customer Data and must not sell any Customer Data as the term "selling" is defined in the CCPA. INK represents and warrants that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from taking any action that would cause any transfers of Customer Data to or from INK to qualify as "selling personal information" under the CCPA.

3.2 Subject to Section 5 of this DPA, where INK processes Customer Personal Data originating from the EEA, the UK and/or Switzerland, and INK transfers such Customer Personal Data to a country not deemed by the European Commission as providing adequate protection for Personal Data, INK warrants and agrees to: (i) comply with its obligations under Applicable Privacy Laws; and (ii) provide at least the same level of protection to Customer Personal Data as is required under this Agreement to ensure an adequate level of protection for Customer Personal Data. INK agrees to notify Customer promptly in writing of its inability to meet its obligations under this Section 3.2 and to take all reasonable and appropriate measures to remedy any non-compliance and/or cease processing Customer Personal Data, as determined by Customer in its sole discretion. INK warrants and agrees to: (i) the SCCs and the clauses to be stipulated according to Art. 28(3) GDPR and where applicable, Art. 28(3) of the UK GDPR, which are both hereby incorporated into this DPA by reference; and (ii) implement the technical and organisational security measures specified in Appendix 2 before processing the Customer Personal Data.

4. Confidentiality and Security

4.1 INK shall ensure that any person that it authorises to process the Customer Data (including INK's staff, agents and subcontractors) shall be subject to a duty of confidentiality.

4.2 INK shall ensure it implements and maintains throughout the term of the Agreement, or duration of its services to Customer as a Processor or Sub-processor, appropriate technical and organisational measures to protect Customer Data, including protection against Data Breaches.

5. Sub-processing

INK shall notify Customer of any Sub-processors it uses in respect of Customer Personal Data, and INK shall: (i) ensure that any Sub-processor is contractually bound in writing to provide at least the same level of protection as is required by this DPA and complies with Applicable Privacy Laws; (ii) be fully responsible for, and liable to Customer for acts and omissions of any Sub-processor as if they were INK's own act or omission; and (ii) provide Customer with details of any Sub-processors appointed, on request. By signing this DPA, Customer authorises INK to use INK current Sub-processors.

6. Cooperation and Data Subjects Rights

INK will provide all assistance reasonably required by Customer to enable Customer to: (i) respond to, comply with or otherwise resolve any rights request, question or complaint received by Customer (or an Customer customer) from: (a) any living individual whose Personal Data is processed by INK on behalf of Customer; or (b) any applicable formally designated data protection authority; and (ii) comply with (and demonstrate compliance with) its obligations under Applicable Privacy Laws. In the event that any such request, question or complaint under this Section 6 is made directly to INK, INK shall inform Customer providing full details of the same unless INK is prohibited by Applicable Privacy Laws.

7. Audit

On reasonable prior written notice and at a time mutually agreed by the parties, at Customer's cost and expense, once per calendar year, INK agrees to provide Customer (or its appointed auditors) with all information Customer deems reasonably necessary for Customer to audit INK's compliance with the requirements of this DPA, including completion of audit questionnaires, provision of security policies and summaries of assessments of compliance with any industry standards (such as ISO 27001, SSAE 16 SOC II), penetration testing and vulnerability scans ("**Audit Information**"). Customer acknowledges that the Audit Information constitutes INK confidential information and it will protect such information in accordance with confidentiality provisions of the Agreement and this DPA. In addition, Customer agrees to leverage existing Audit Information provided by INK to the extent such documentation satisfies the requirements of Article 28 of the GDPR.

8. Data Breach

In the event of a Data Breach, INK will take only the following actions (unless authorised by Customer):

8.1 promptly notify Customer without undue delay (and latest within 48 hours of becoming aware of the Data Breach) and provide Customer with a reasonably detailed description of the Data Breach, the type of data that was

the subject of the Data Breach and the identity of each affected person as soon as such information can be collected or otherwise becomes available, as well as any other information that Customer may reasonably request relating to the Data Breach; and

8.2 promptly investigate the Data Breach, make reasonable efforts to mitigate the effects and harm of the Data Breach in accordance with its obligations under Section 4 (Confidentiality and Security) above, and provide any other assistance that Customer may reasonably request relating to the Data Breach.

9. Deletion or Return of Data

Upon termination or expiration of this DPA, INK shall (at Customer's election) destroy or return to Customer all Customer Data (including all copies of Customer Data) in its possession or control (including any Customer Data subcontracted to a third party for processing), unless any applicable law requires INK to retain Customer Data.

10. Indemnity

INK will indemnify, keep indemnified and hold harmless Customer, its clients, officers, directors, employees, agents, representatives and Affiliates (each an "**Indemnified Party**") from and against all third-party loss, harm, cost (including reasonable legal fees and expenses), expense and liability that an Indemnified Party may suffer or incur as a result of INK's non-compliance with the requirements of this DPA but solely to the extent that INK fails to act or acts outside or against the instructions of Customer. INK's liability under this Agreement shall be limited to the amount paid by Customer to INK in the previous year.

11. International Data Transfers

11.1 **EEA Transfers**. With respect to Customer Personal Data transferred from the European Economic Area ("**EEA**"), the New EU SCCs shall apply, form part of the DPA, and take precedence over the rest of the DPA to the extent of conflict. If and to the extent a Customer Affiliate relies on the New EU SCCs for the transfer of Customer Data, any reference to Customer includes such Customer Affiliate. Where INK is acting as Customer's Processor, Module Two of the New EU SCCs shall apply. Where INK is acting as Customer's Sub-processor, Module Three of the New EU SCCs shall apply. For both Modules Two and Three, Customer is the Data Exporter and INK is the Data Importer. INK hereby agrees to enter into the New EU SCCs, which are incorporated into this DPA by this reference and completed as follows:

i. In Clause 7, the Parties choose not to include the optional docking clause.

ii. In Clause 9, the Parties select the Option 2 (General Written Authorization) and provide for a 30-day advance notice.

iii. In Clause 11, the Parties choose not to include the optional language relating to the use of an independent dispute resolution body.

iv. In Clauses 17 and 18, the Parties choose the law of the Republic of Ireland and the courts of the Republic of Ireland.

v. Annexes. The Parties agree that Annex I and Annex II shall be as set forth in the Appendix 2 to this DPA.

11.2 **UK Transfers**. With respect to Customer Personal Data transferred from the United Kingdom for which the United Kingdom law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, the UK SCC Addendum forms part of the DPA and takes precedence over the rest of the DPA as set forth in the UK SCC Addendum, unless the United Kingdom issues updates to the UK SCC Addendum, in which case the updated UK SCC Addendum will control.

INK hereby agrees to enter into the UK SCC Addendum, which is incorporated into this DPA by this reference and completed as follows:

i.Table 1: The content of Table 1 is set forth in the Agreement and this DPA.

Table 2: The content of Table 2 is set out in this DPA. The Parties agree that Modules two, three and four of the New EU SCCs are applicable. To the extent that Module four is applicable, the Parties confirm that Personal Data received from the Data Importer [is][is not] combined with personal data collected by the Data Exporter.

Table 3: The applicable content of Table 3 (Annex 1(A), 1(B), II, and III) is set forth as follows:

(A) Annex 1(A): The content of Annex 1 (A) is set forth in the Agreement and DPA.

(B) Annex 1(B): The content of Annex 1 (B) is set forth in the DPA and Appendix 1 thereto.

(C) Annex II: The content of Annex III is set forth in the DPA and Appendix 2 thereto.

(D) Annex III: The content of Annex III is set forth in the DPA and Appendix 1 thereto.

Table 4: The Parties agree that neither Party may terminate the UK Transfer Addendum.

3 **Switzerland Transfers**. With respect to Customer Personal Data transferred from Switzerland for which Swiss law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, (i) references to the

GDPR in Clause 4 of the New EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner; and (ii) as so amended, the New EU SCCs are incorporated herein by reference and shall apply, form part of this DPA, and take precedence over the rest of this DPA to the extent of conflict.

11.4 Transfer Assessment. To the extent required under or necessitated by Applicable Privacy Laws and/or guidance issued by data protection regulatory authorities in relevant jurisdictions, INK shall conduct a risk assessment of any such international transfer to determine if the level of protection provided under the laws of the recipient country are adequate to protect the Customer Personal Data in advance of engaging in any such transfer ("**Transfer Assessment**"). Depending on the outcome of any such Transfer Assessment, INK shall implement additional measures as necessary to ensure the protection of the Customer Personal Data, which may include, without limitation, additional contractual protections and security measures. Upon Customer's reasonable request, INK shall provide Customer with information to enable Customer to complete its own such assessments.

12. Miscellaneous

Except for the changes made by this DPA, the Agreement and/or any other agreements related to the Services remain unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Agreement or other agreements between the parties, this DPA controls and takes precedence.

[SIGNATURES BELOW]

IN WITNESS WHEREOF, the Parties have caused this DPA to be executed by their authorised representative effective as of the DPA Effective Date.

<<CUSTOMER NAME>>	**INK CONTENT , INC.**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1

Data Processing Description

I. List of the Parties

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

Customer Name: _____

Address: _____

_____

Contact person's name, position and contact details: As provided under the Agreement between data exporter and data importer.

Activities relevant to the data transferred under these Clauses: Transferring and accessing the data and any other activities related to receipt of the Services described under the Agreement.

Signature and date: The data exporter's signature to the DPA and date of that signature shall constitute the signature and date for this Appendix.

Role (controller/processor): For purposes of Module 1 of the Standard Contractual Clauses, data exporter is the Data Controller. For purposes of Module 2 of the Standard Contractual Clauses, data exporter is the Processor.

Data importer(s): INK Content, Inc.

Address and contact person information shall be as set out under the Agreement between the data exporter and data importer.

Activities relevant to the data transferred under these Clauses: Processing in order to provide the Services to Customer as described in the Agreement between data exporter and data importer, including as described under the DPA and its appendices.

Signature and date: The data importer's signature to the DPA and date of that signature shall constitute the signature and date for this Appendix.

Role (controller/processor): Processor.

II. Description of Transfer

a. Subject matter, nature, and purpose of Processing: INK will process Customer Personal Data solely to fulfil its purposes under the Agreement, including Processing Personal Data: (i) to provide the Service in accordance with the Agreement; (ii) to perform any steps necessary for the performance of the Agreement; (iii) to perform any Processing activity initiated by Customer in its use of the Service; and (iv) to comply with other reasonable instructions provided by Customer that are consistent with the terms of the Agreement and this DPA.

b. Duration of the Processing: For the term of the Agreement plus the period from expiration or termination of the Agreement until deletion of all Customer Personal Data by INK in accordance with the Agreement.

c. Categories of Data Subjects: Data subjects may include Customer's representatives, such as employees, contractors, collaborators, partners or any other individuals about whom data is provided to INK via the Service by (or at the direction of) Customer or its Users.

d. Special Categories of Customer Personal Data to be Processed (if applicable) and the applied restrictions to the Processing of these Special Categories of Customer Personal Data: N/A. INK does not intentionally collect or Process any special categories of Personal Data.

e. Categories of Personal Data typically subject to Processing under the Agreement: The categories of Customer Personal Data that Customer authorises and requests that INK Processes and include data relating to individuals provided to INK via the Service, by (or at the direction of) Customer or its Users; for example, in the text in electronic form submitted to the Service.

f. Categories of third-party recipients to whom the Customer Personal Data may be disclosed or shared by INK: Subprocessors and INK Affiliates, if applicable.

g. Frequency of the Transfer of Customer Personal Data: The frequency of the transfer of Customer Personal Data is determined by the Customer. Customer Personal Data is transferred each time that the Customer instructs INK to Process Customer Personal Data.

h. Maximum data retention periods, if applicable: The retention period of the Customer Personal Data is generally determined by the Customer and is subject to the terms of the DPA and the Agreement, respectively, in the context of the contractual relationship between INK and the Customer.

i. The basic Processing activities to which Customer Personal data will be subject include, without limitation: Collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Services to Customer in accordance with the terms of the Agreement.

j. The following is deemed an instruction by the Customer to INK to Process Customer Personal Data:

    a. Processing in accordance with the Agreement;

    b. Processing initiated by Data Subjects in their use of the Services; and

    c. Processing to comply with other reasonable documented instructions provided by Customer (e.g. via email) where such instructions are consistent with the terms of the Agreement.

k. List of INK's Subprocessors is available at https://smythos.com/legal/subprocessors/ .

Appendix 2

Technical and Organisational Security Measures

References to 'data importer' in this Appendix 2 means INK.

Policies for information security: The data importer agrees to implement a set of policies for information security that are defined, approved by management, published and communicated to employees and relevant external parties.

Review of the policies for information security: The data importer agrees to ensure that the policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Information security awareness, education and training: The data importer will ensure all employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

Acceptable use of assets: The data importer will ensure rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

Classification of information: The data importer will ensure all information assets are classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Disposal of media: The data importer will ensure all media is disposed of securely when no longer required, using formal procedures.

Access control policy: The data importer will ensure an access control policy is established, documented and reviewed based on business and information security requirements.

Policy on the use of cryptographic controls: The data importer will ensure a policy on the use of cryptographic controls for protection of information has been developed and implemented.

Physical security perimeter: The data importer will ensure that security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Physical entry controls: The data importer will ensure secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

Secure disposal or reuse of equipment: The data importer will ensure all items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Controls against malware: The data importer will implement detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Information backup: The data importer will implement a backup policy to define the organisation's requirements for backup of information, software and systems.

Management of technical vulnerabilities: The data importer will action technical vulnerabilities mitigation, to reduce exposure to such vulnerabilities and ensure appropriate measures are taken to address the associated risk.

Information systems audit controls: The data importer will implement audit requirements and activities involving verification of operational systems to ensure carefully planned and agreed to minimise disruptions to business processes.

Network controls: The data importer will ensure Networks are managed and controlled to protect information in systems and applications and ensure groups of information services, users and information systems are appropriately segregated.

Electronic messaging: The data importer will ensure information involved in electronic messaging will be appropriately protected.

Confidentiality or non-disclosure agreements: The data importer will ensure requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information are identified, regularly reviewed and documented.

Securing application services on public networks: The data importer will ensure information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

Secure system engineering principles: The data importer will ensure principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.

System security and acceptance testing: The data importer will ensure testing of security functionality is carried out during development and that acceptance testing programs and related criteria are established for new information systems, upgrades and new versions. The data importer will ensure test data is selected carefully, protected and controlled.

Reporting and responding to information security events: The data importer will ensure Information security events are reported through appropriate management channels as quickly as possible and will ensure information security incidents are responded to in accordance with the documented procedures.

Planning information security continuity: The data importer will determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.