WISETAIL DATA PROCESSING AGREEMENT ("DPA")

The customer agreeing to the terms of this DPA ("**Customer**") and Bigart Ecosystems, LLC ("**Wisetail**"; each of Customer and Wisetail a "**Party**" and collectively the "**Parties**"), have entered into an agreement (such as the Wisetail Terms of Service and Order Form) governing Customer's use of Wisetail LMS System, including the Service, and the provision of related Professional Services to Customer by Wisetail, including any attachments, order forms, exhibits, and appendices thereto (collectively, the "**Agreement**"). This DPA supplements, is incorporated into, and forms part of the Agreement and establishes the rights and obligations of Wisetail and Customer with respect to any Customer Personal Data Processed by Wisetail on behalf of Customer under the Agreement. Any capitalized terms used but not defined in this DPA shall have the meaning provided in the Agreement. To the extent there is any conflict in meaning between any provisions of the Agreement and this DPA, the terms and conditions in this DPA shall prevail and control.

1. DEFINITIONS

1.1 The following capitalized terms will have the meanings indicated below:

- "**Adequate Country**" means a country that may import Personal Data and is deemed by the governing authority of the exporting country to provide an adequate level of data protection under the applicable Data Protection Laws;
- "**Affiliate**" means an entity that, directly or indirectly, owns or controls or is owned or controlled by, or is under common ownership or control with, a Party. As used herein, "control" means the power to direct, directly or indirectly, the management or affairs of an entity and "ownership" means the beneficial ownership of more than fifty percent of the voting equity securities or other equivalent voting interests of an entity.
- "**Completions**" has the meaning given to it in Exhibit D of this DPA;
- "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data and includes, as applicable, the term "controller" "business" and any other similar or equivalent terms under applicable Data Protection Laws;
- "**Customer Personal Data**" means any Personal Data contained within Customer Data subject to Data Protection Laws that Customer, including Users, provides or makes available to Wisetail in connection with the Agreement;
- "**Data Incident**" means any breach, as defined by applicable Data Protection Laws, of Wisetail's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data on systems managed or otherwise controlled by Wisetail;
- "**Data Protection Authority"** means a competent authority responsible for enforcing the application of the relevant Data Protection Laws, and includes, as applicable, any data protection authority, privacy

regulator, supervisory authority, Attorney General, state privacy agency or any governmental body or agency enforcing Data Protection Laws;

- **"Data Protection Laws**" means all laws and regulations as amended from time to time regarding data protection, consumer privacy, electronic communications and marketing laws to the extent applicable to the Processing of Customer Personal Data by Wisetail under the Agreement, such as:
    - California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**");
    - California Privacy Rights Act of 2020 ("**CPRA**");
    - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**EU GDPR**");
    - The EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and
    - The Switzerland Federal Data Protection act of 19 June 1992 as replaced and/or updated from time to time ("**FDP**").
- "**Data Protection Officer**" means the natural person or company appointed where necessary under applicable Data Protection Laws to ensure an organization's compliance with Data Protection Laws and cooperate with the Data Protection Authorities;
- "**Data Subject**" means the identified or identifiable person to whom Personal Data relates, and includes, as applicable, the term "consumer" and any other similar or equivalent terms under Applicable Data Protection Laws;
- "**DPA Effective Date"** means the Effective Date of the Agreement;
- "**EEA**" means the European Economic Area;
- "**EU SCCs**" means the standard contractual clauses for use in relation to exports of Personal Data from the EEA approved by the European Commission under Commission Implementing Decision 2021/914, or such other clauses as replace them from time to time;
- "**Personal Data**" means: (a) any information relating to (i) an identified or identifiable natural person and/or (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws), and (b) any information treated or receiving similar treatment as "personal data", "personal information", "personally identifiable information or any similar, or equivalent terms under applicable Data Protection Laws;
- "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms "process", "processes" and "processed" will be interpreted accordingly;
- "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as

applicable the terms “processor”, “service provider” and any equivalent or similar terms that address the same, or similar, responsibilities under applicable Data Protection Laws;

- “**Request**” means a request from a Data Subject or anyone acting on their behalf to exercise their rights under Data Protection Laws;
- “**Restricted Transfer**” means a transfer, or onward transfer, of Personal Data from a country where such transfer would be restricted or prohibited by applicable Data Protection Laws (or by the terms of a data transfer agreement put in place to address the data transfer restrictions of Data Protection Laws) without implementing safeguards such as the Standard Contractual Clauses to be established under clause 14 below;
- “**Security Documentation**” means the Documentation describing the security standards that apply to the Service as provided by or on behalf of Wisetail from time to time;
- “**Sell**” or “Sale” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject’s Personal Data to a third party for valuable consideration.
- “**Service**” shall have the meaning as set out in the Agreement and this DPA.
- **“Share”** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject’s Personal Data to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions in which no money is exchanged;
- “**Subprocessor**” means any processor or service provider who processes personal data on behalf of Wisetail for the purpose of providing the Service as set out in the Agreement, Exhibit A and any other relevant applicable exhibits of this DPA.
- “**Standard Contractual Clauses**” or “**SCCs**” means either (a) the standard data protection clauses approved pursuant to the Data Protection Laws of the applicable exporting country from time to time to legitimize exports of Personal Data from that country, or (b) where the applicable exporting country has Data Protection Laws that regulate the export of personal data but no approved standard data protection clauses, the EU SCCs shall apply- in each case incorporating the appropriate Completions, and where more than one form of such approved clauses exists in respect of a particular country, the clauses that shall apply shall be: (i) in respect of any situation where Customer acts as a Controller of Customer Personal Data, that form of clauses applying to Controller to Processor transfers; and (ii) in respect of any situation where Customer acts as a Processor of Customer Personal Data, that form of clauses applying to Processor to Processor transfers; and
- “**Technical and Organizational Measures**” means the technical and organizational measures agreed by the Parties in the Agreement and any additional technical and organizational measures implemented by Wisetail pursuant to its obligations under applicable Data Protection Laws.

2. TERM

2.1 This DPA will take effect from the DPA Effective Date and remain in effect until the destruction or return of

all Customer Personal Data by Wisetail in accordance with the Agreement, at which point it will automatically terminate.

3. SCOPE AND APPLICATION

3.1 This DPA is incorporated into, and forms part of, the Agreement and establishes the rights and obligations of Wisetail and Customer with respect to any Customer Personal Data Processed by Wisetail on behalf of Customer when in the course of the provision of the Service. To the extent there is any conflict in meaning between any provisions of the Agreement and this DPA, the provisions in this DPA shall prevail and control.

4. ROLE OF THE PARTIES

4.1 Customer and any relevant Customer Affiliate, hereby appoints and instructs Wisetail as a Processor, or Sub-Processor as applicable, of the Customer Personal Data. Accordingly, the Parties shall comply with applicable Data Protection Laws as relevant to their respective Processing of Customer Personal Data under the Agreement.

4.2 As between the Parties, Customer shall be liable and responsible as the Controller (or Processor, if Customer is Processing Personal Data with the Service for a third party Controller) and Wisetail shall be liable and responsible as the Processor (or Subprocessor), in respect of Customer Personal Data. In the event that Customer acts as a Processor (or Subprocessor) in respect of Customer Personal Data, Customer represents and warrants to Wisetail that it is validly authorized by the relevant Controller to enter into the Agreement and this DPA and to provide Customer Instructions (as defined below) on behalf of the Controller in relation to Customer Personal Data.

4.3 The subject matter and details of Processing are described in the Agreement and this DPA, including Exhibit B (subject matter and details of Customer Personal Data processing) and any other relevant exhibits for applicable additional Services.

5. CUSTOMER PROCESSING OF PERSONAL DATA

5.1 Customer shall ensure that any Processing of Customer Personal Data via Customer's use of the Service, including any instructions provided to Wisetail in relation to such Processing, shall comply with all applicable Data Protection Laws.

5.2 Customer instructs Wisetail to Process Customer Personal Data: (a) to provide the Service specified in the Agreement and Documentation or otherwise perform its obligations thereunder; (b) as further initiated by Customer via Customer's or Users use of the Service in accordance with the Agreement and Documentation; and/or (c) in accordance with any additional instruction outside the scope of the Agreement or this DPA, as further documented in any other written instructions given by Customer and acknowledged by Wisetail in writing as constituting instructions for purposes of this DPA (collectively, "Customer Instructions"). Customer acknowledges that any additional Customer Instructions issued under (c) above may result in additional charges or fees to the Customer by Wisetail, which shall be payable in accordance with the terms of the Agreement.

5.3 Customer shall have sole responsibility for the lawful Processing of Customer Personal Data in connection with its use of the Wisetail LMS System and/or its receipt of any related Professional Services in accordance with applicable Data Protection Laws, including without limitation, the accuracy, quality, and legality of the Customer Personal Data, the means by which it acquires and uses Customer Personal Data, and the

Customer Instructions regarding the Processing of Customer Personal Data. Customer represents and warrants that it has (or its Controller has) a valid legal basis for the Processing of Customer Personal Data and has (or its Controller has) provided (or procured the provision of) all notifications and obtained (or procured the provision of) all consents (including Consents), authorisations, approvals, and/or agreements (including, where Customer is a Processor or Subprocessor, with and from the applicable Controller(s)) required under applicable laws or policies in order to enable Wisetail to receive and Process Customer Personal Data in accordance with this DPA, the Agreement and Customer Instructions.

6 . WISETAIL PROCESSING OF CUSTOMER PERSONAL DATA

6.1 Wisetail will Process Customer Personal Data for the business purposes of providing to Customer the services, namely the Wisetail LMS System and Professional Services pursuant to the Customer Instructions ("Business Purposes"), in accordance with the terms of the Agreement and this DPA as well as any requirements set out by applicable Data Protection Laws. For the avoidance of doubt, Customer is disclosing Customer Personal Data to Wisetail only for the limited and specified Business Purposes set forth within the Agreement and the Customer Instructions. Wisetail shall process Customer personal Data pursuant to Customer's instructions and shall:

(a) designate and maintain a Data Protection Officer as required by Data Protection Laws as they pertain to Processors, Adrian Brown, which can be contacted at security.office@wisetail.com;

(b) not Sell or Share Customer Personal Data or otherwise retain, use, disclose, or Process Customer Personal Data outside of the direct business relationship between the Parties or for any purpose other than for the fulfilment of the Business Purposes pursuant to Customer Instructions, unless obligated to do otherwise by applicable law or regulation or requests or orders of judicial, governmental or regulatory entities (including without limitation subpoenas), in which case Wisetail will inform Customer of that legal requirement before such Processing occurs unless legally prohibited from doing so;

(c) not combine Customer Personal Data with Personal Data that it receives from other sources or collects from its own interactions with a Data Subject, provided, however, that Wisetail may combine Customer Personal Data as necessary to perform its internal business purposes in connection only with the provision of the Service;

(d) implement appropriate Technical and Organizational Measures as described in the Security Documentation to ensure a level of security appropriate to the risk against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, 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. To the extent such assistance requires Wisetail to take additional steps beyond those imposed on Wisetail by Data Protection Laws or specifically required pursuant to the Agreement; or to the extent the relevant technical and organizational measures are required as a result of an act or omission by Customer or a Party acting on behalf of Customer in breach of this Agreement or Data Protection Laws, then Wisetail's obligation to provide such assistance shall be subject to Customer's payment of Wisetail's reasonable fees in respect of such additional assistance;

(e) ensure that all persons authorized by Wisetail to Process Customer Personal Data, including any Subprocessors (as defined below), are bound by confidentiality obligations consistent with those set out

in this DPA, the Agreement or otherwise sufficient to meet the requirements of Data Protection Laws;

(f) take reasonable steps to return or destroy Customer Personal Data at the choice of the Customer, when it is no longer necessary for the purposes of performing the relevant Services upon termination of the Agreement, unless storage is otherwise required under applicable Data Protection Laws; and

(g) process Customer Personal Data in a manner that is consistent with the same level of privacy protection that is required of Customer under applicable Data Protection Laws.

6.2. Customer shall instruct Wisetail as to the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects taking into account the specific tasks and responsibilities of the Processor in the context of the Processing to be carried out and the risk to the rights and freedoms of the Data Subject as part of Customer Instructions. Notwithstanding anything to the contrary herein, Customer shall ensure that its acts or omissions, including in relation to any Customer Instructions to Wisetail, do not put Wisetail in breach of the Data Protection Laws.

6.3 Customer has assessed the level of security appropriate to the Processing in the context of its obligations under Data Protection Laws and agrees that the Technical and Organizational Measures are consistent with such assessment. Customer further acknowledges that Wisetail is not able to assess, and does not have knowledge of, the specific Personal Data provided by Customer to Wisetail or made available by Customer to Wisetail in relation to the Services and that as a result the technical and organizational Measures proposed by Wisetail are generic in nature and Wisetail is unable to assess whether or not they reflect any particular risks posed by the Personal Data.

7. SUBPROCESSORS

7.1 Customer specifically authorizes the engagement as Subprocessors of (a) the entities listed in Exhibit A and/or applicable specific additional Services exhibits in this DPA and (b) all Wisetail Affiliates from time to time, provided that, prior to permitting such Subprocessors to Process any Customer Personal Data, Wisetail shall enter into a written agreement with the Subprocessor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

7.2 Subject to Section 7.3, Customer generally authorizes Wisetail to engage additional Subprocessors ("**Additional Subprocessors**"), provided that, prior to permitting such Additional Subprocessor to Process any Customer Personal Data, Wisetail shall enter into a written agreement with the Additional Subprocessor imposing terms that are consistent with those set out in this DPA or otherwise sufficient to meet the requirements of Data Protection Laws.

7.3 Should Wisetail engage an Additional Subprocessor, it shall provide Customer with no less than 30 days' notice, including the identity, location, and nature of Processing proposed to be undertaken by such Additional Subprocessor. That notice with be given by email notification and the customer will have the right to approve or reject the Additional SubProcessor. Where Customer indicates in writing that it objects to the Processing of Customer Personal Data by such Additional SubProcessor, the Parties shall seek to resolve the Customer concerns and where necessary the Customer may exercise its applicable rights to terminate the Agreement.

7.4 To the extent required by Data Protection Law, Wisetail shall remain liable to Customer for the performance of the Subprocessor's obligations in relation to this Section 7 ("**Subprocessor Data Protection Liability**"), and Wisetail shall be permitted to re-perform or to procure the re-performance of any such obligations and

Customer acknowledges that such re-performance shall diminish any claim that Customer has against Wisetail in respect of any Subprocessor Data Protection Liability.

8. AUDIT

8.1 Wisetail uses third party auditors to verify the adequacy of its security measures. This audit is performed at least annually, by independent and reputable third-party auditors at Wisetail's selection and expense, and in accordance with Service Organization Controls 2 (SOC2) or substantially equivalent industry standards, and results in the generation of an audit report ("Report") which will be the Confidential Information of Wisetail. Subject to a mutual non-disclosure agreement between the Parties, the Report can be requested by Customer.

8.2 At Customer's written request, Wisetail will provide Customer with a confidential summary of the Report, documentation evidencing compliance with the Accreditations, and the Accountability Information outlined in Section 10 of this DPA so that Customer can reasonably verify Wisetail's compliance with the data security and data protection obligations under this DPA. Subject to Section 8.3, if Data Protection Laws, Standard Contractual Clauses, or the Agreement require Wisetail to provide Customer with information in addition to the Report and the Accountability Information, then Wisetail shall permit Customer to audit, subject to mutual agreement as to timing and scope, Wisetail's compliance with the terms and conditions of this DPA as it applies to Customer Personal Data to the extent expressly required by the Agreement, the Standard Contractual Clauses, or Data Protection Laws.

8.3 All information provided or made available to Customer, its auditor or any other third-party authorized under the present DPA to have access to the above information pursuant to this Section 8 shall be Confidential Information of Wisetail.

8.4 In the event of any confirmed material non-compliance by Wisetail with the terms of this DPA, Customer may take reasonable steps to remediate the same, including, without limitation, by requiring the suspension of all Processing of Customer Personal Data until such time as Customer determines that the non-compliance has been remediated. In the event that Wisetail determines that it can no longer meet its obligations pursuant to this DPA, Wisetail shall promptly notify Customer of such determination.

9. DEALINGS WITH DATA PROTECTION AUTHORITIES AND DATA PROTECTION IMPACT ASSESSMENTS

9.1 Wisetail shall reasonably cooperate, on reasonable request and at Customer's cost, with any Data Protection Authority in the performance of its tasks, taking into account the nature of the Processing by, and information available to, Wisetail.

9.2 Taking into account the nature of the Service and the information available to Wisetail, Wisetail will assist Customer in complying with Customer's obligations in respect of data protection impact assessments (including a 'risk assessment', 'privacy impact assessment', 'data protection assessment' or any equivalent documentation) and prior consultation or mandatory submission to a Data Protection Authority where applicable under Data Protection Laws, by providing the Report, Accountability Information and Documentation.

10. ACCOUNTABILITY

10.1 To the extent required by Data Protection Laws, Wisetail shall maintain electronic records of all categories of Processing activities carried out on behalf of Customer, containing:

(a) the name and contact details of the Processors and Subprocessors;

(b) details of the types of Processing being carried out;

(c) details of any transfers of Customer Personal Data to a territory or international organisation outside of the EEA or UK, and documentation of suitable safeguards (if applicable); and

(d) a general description of the technical and organizational security measures used in relation to the Processing,

together, the "**Accountability Information**".

11. DATA SUBJECT RIGHTS

11.1 With regard to Customer Personal Data, where Wisetail directly receives a Request from a Data Subject, or anyone authorized to act on their behalf, any claim or complaint in relation to their rights under the Data Protection Laws, and provided Wisetail can reasonably identify from the information provided that the request, claim or complaint relates to Customer and Customer Personal Data, then unless prohibited by applicable law, Wisetail shall forward the request, claim or complaint to Customer. Customer, not Wiestail, will be responsible for deleting Personal Data on behalf of Data Subject.

11.2 On reasonable written request from Customer, and taking into account the nature of the Processing, Wisetail shall use commercially reasonable efforts to offer Customer certain controls as described in the Documentation that Customer may elect to use to comply with its obligations towards Data Subjects.

12. DATA INCIDENT

12.1 Wisetail shall notify Customer without undue delay after becoming aware of (or where required by applicable Data Protection Laws) a Data Incident and provide Customer with any information required to be included under applicable Data Protection Laws. For avoidance of doubt, a Data Incident shall not include acts or omissions which do not breach Wisetail's security or the security of any Subprocessor; port scans, authorized penetration tests, and denial of service attacks; or any access to or Processing of Customer Personal Data that is consistent with Customer Instructions.

12.2 Wisetail shall provide Customer with reasonable cooperation and assistance in dealing with a Data Incident, in particular in relation to (a) taking commercially reasonable steps to resolve any data privacy or

security issues involving any Customer Personal Data; and (b) making any appropriate notifications to individuals affected by the Data Incident or to a Supervisory Authority to the extent reasonably possible; provided that, Customer shall maintain and follow an effective cyber incident response policy, which shall include the use of legal professional, litigation, or client attorney privilege, work in good faith with Wisetail in relation to the Data Incident, and agree with Wisetail the form and method of any public announcement in relation to the Data Incident.

12.3 Any information provided by Wisetail pursuant to this Section 12 shall be the Confidential Information of Wisetail and Wisetail's notification of or response to a Data Incident under this Section 12 will not be construed as an acknowledgement by Wisetail or, if relevant, its Subprocessors of any fault or liability with respect to the performance of any Service or Professional Services (as applicable).

13. DATA TRANSFERS

13.1 Wisetail may Process Personal Data in countries outside of the country in which Customer is established in which Wisetail or its Subprocessors maintains facilities, employees or infrastructure. Wisetail's primary place of business and Processing is the United States.

13.2 Where the Processing of Customer Personal Data in the course of the provision of the Service involves a Restricted Transfer of Customer Personal Data by or on behalf of Customer, from a country which places restrictions on the transfer of Personal Data to countries not deemed to be an Adequate Country then:

(a) Wisetail shall provide appropriate safeguards, meeting the requirements of the applicable SCCs in respect of onward transfers, in relation to transfers of the Personal Data between Wisetail Affiliates for the purpose of performing Services; and

(b) Wisetail shall ensure that any transfers of Customer Personal Data between Wisetail and any Wisetail third party Subprocessors, are subject to contractual terms between Wisetail and the relevant third party Subprocessor providing appropriate safeguards and containing clauses equivalent to the SCCs; or

(c) Where the Parties choose to enter into SCCs, the applicable SCCs and any required Completions as applicable and set out in Exhibit D, shall hereby be deemed incorporated into this DPA, and apply between Customer (as Exporter) and Wisetail (as importer),

13.3 Nothing in this DPA or the Agreement modifies any rights or obligations of Wisetail or customer under the Standard Contractual Clauses.

14. LIABILITY

14.1 Subject to 14.2, the total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or in connection with the Agreement and the Standard Contractual Clauses combined will be the liability cap, and subject to the liability limitations, set forth in the Agreement for the relevant Party.

14.2 Nothing in this DPA serves to modify, disapply or amend the terms of the Agreement relating to liability, including but not limited to any exclusions and/or limitations of liability.

14.3 Customer shall ensure that all Customer Data it uploads in the course of the provision of the Service is accurate and complies with all applicable laws. Wisetail does not monitor or control any Customer Data on Wisetail Services. Customer shall defend and indemnify Wisetail for any and all damages, liabilities, penalties, fines and expenses (including from third parties) arising out of the Customer's failure to comply with the present provision or any applicable laws in connection with Customer Data.

15. GOVERNING LAW AND JURISDICTION

15.1 The Parties shall modify the terms of this DPA as soon as possible if such modification is required for the parties to comply with any Data Protection Laws, or in order to implement or adhere to the Standard Contractual Clauses or such other permitted compliance mechanism under Data Protection Laws.

15.2 This DPA, and any dispute or claim (including any non-contractual disputes or claims) arising out of or in connection with it, or its subject matter or formation, shall be governed by and construed in accordance with the laws that govern the Agreement. If it is or becomes a requirement that, under the Data Protection Laws or other applicable laws, this DPA must be governed by (a) the laws of a member state of the European Union (and it is not already so governed), this DPA shall be governed by and construed in accordance with the laws of Ireland; (b) the laws of the United Kingdom, this DPA shall be governed by and construed in accordance with the laws of England and Wales, and/or (c) the laws of any other jurisdiction, then this DPA shall be governed by and construed in accordance with the laws of that jurisdiction, but only to the extent required to satisfy such laws.

15.3 The Parties irrevocably agree that the forum set out in the Agreement shall have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this DPA and the documents to be entered into pursuant to it and that, accordingly, any proceedings arising out of or in connection with this DPA shall be brought in such forum save that where a mandatory requirement of Data Protection Law or other applicable laws requires that disputes arising out of or in connection with this DPA and any documents to be entered into pursuant to it are heard in (a) a member state of the European Union, then such disputes shall be heard in Ireland; (b) the United Kingdom, then such disputes shall be heard in England and Wales; and/or (c) any alternative forum, then such disputes shall be heard in that alternative forum, to the extent legally permitted. Each of the Parties irrevocably submits to the jurisdiction of such forum and waives any objection to proceedings in any such forum on the ground of venue or on the ground that proceedings have been brought in an inconvenient forum.

16. GENERAL TERMS

16.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, whilst preserving the Parties' intension as closely as possible, or, where not possible, (ii) construed in a manner as if the invalid off unenforceable part had never been contained therein.

16.2 Wisetail may notify Customer in writing from time to time of any variations to this DPA, including relating to cross border transfers, which are required as a result of change in Data Protection Laws.

EXHIBIT A

List of approved Subprocessors

To perform its obligations under the Agreement and DPA, Wisetail may use third-party data processors ("**Third-Party Subprocessors**") and Affiliates to process Customer Personal Data. Capitalized terms used but not defined here shall have the meanings provided in the Agreement.

The following third parties are hereby specifically authorized by Customer to carry out work as Third-Party Subprocessors for purposes of the Agreement:

Name	Processing
Amazon Web Services	Cloud Service Provider
Splunk	Log and Security Data
JW Player	Video Player in the Platform
Filestack	Upload Manager for Content
Twilio	User Notifications
Mailgun	System Email Repository
Github	Source Code Repository
Encoding.com	Video Transcoding
Pendo	Application Performance Monitoring
Merge	System Integrator
Google Firebase	Push Notifications

PART II – Wisetail Affiliates

Provided that an adequate level of data protection consistent with the Data Protection Laws and this Agreement is ensured by Wisetail, Customer specifically authorizes Wisetail Affiliates as listed here and as updated from time to time to act as Wisetail's Subprocessor(s) including by Processing Customer Personal Data for the purposes of the Agreement for the delivery of Service and/or Professional Services to Customer. Where required, Wisetail and its respective Affiliate have entered into the Standard Contractual Clauses. Such Processing, where applicable, shall occur under the control and direction of Wisetail and shall occur on systems managed or otherwise controlled by Wisetail.

1. PlayerLync LLC

2. Frameworks Inc.

EXHIBIT B

Subject Matter and Details of Customer Personal Data Processing

Description of Data Processing / Transfer

This Annex A forms part of the Agreement and describes the processing that Wisetail will perform on behalf of Client.

A. LIST OF PARTIES

Data exporter:

1.	**Name:**	Bigart Ecosystems, LLC
	Address:	117 E. Oak St. Suite 2a, Bozeman, MT 59715
	Contact person's name, position and contact details:	Adrian Brown, IT Manager & Cyber Security Analyst, Security.office@wisetail.com
	Activities relevant to the data transferred under these Clauses:	*As described in Section B below*
	Signature and date:	*Deemed executed when this Agreement is executed by* Wisetail.
	Role (controller/processor):	*Sub-processor*

Data importer:

1.	**Name:**	
	Address:	
	Contact person's name, position and contact details:	
	Activities relevant to the data transferred under these Clauses:	*As described in Section B below*
	Signature and date:	*Deemed executed when the Agreement is executed by Client.*
	Role (controller/processor):	*Processor*

B. DESCRIPTION OF TRANSFER: Client defines data to be transferred

Categories of data subjects whose personal data is transferred:	Customer Employees
Categories of personal data transferred:	First Name, Last Name, Company email / personal email, Franchisee or Employee Information such as Title and Location, Region, Employee ID, and other applicable company or employee information. Categories of Personal data are Client defined and can be reduced as necessary for desired site functionality.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	**NA**

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	*Data is transferred in multiple ways with the most frequent data transfer occurring daily. Below are the different possible methods for data transfer:* *- The transfer is handled via a Client Datafeed from an HRIS. The frequency is daily.* *-The transfer is handled by delegating user provisioning abilities to franchise owners. Data will be manually transferred on an as needed basis.* *- The transfer is handled by a single sign on (SSO) integration. Data will be automatically transferred on an as needed basis.*
Nature of the processing:	*Facilitating access to training content & Client Tracking or reporting for business operations.*
Purpose(s) of the data transfer and further processing:	*Facilitate training access for employees and facilitate training and compliance tracking by Client.*
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	*Data will be retained only for the purposes of Client and its Franchisees to facilitate training. Client has the ability to add or remove personal data at any time or upon request from the data subject (or instruction from its Franchisee). Upon termination of the agreement between Wisetail and Client no data will be retained.*
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	*All data is processed through Amazon Web Services (AWS). Any further data transferred to a sub-processor only includes First and Last Name, Email Address, IP Address, or a unique identifier such as username necessary for LMS functionality.*

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	*For the EU (where applicable) the competent supervisory authority shall be determined in accordance with clause 13 of the EU SCCs. For the UK, the competent supervisory authority is the United Kingdom Information Commissioner's Office.*

EXHIBIT C

Technical and Organizational Security Measures

Description of the technical and organizational security measures implemented by Wisetail 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 in accordance with Section 5 of this DPA.

Type of measure	Description"
Measures of pseudonymisation and encryption of personal data	Wisetail employs encryption measures to protect personal data, through the use of TLS 1.2 or greater, HTTPS, and RSA-2048 encryption. We also ensure encryption of data at rest. Our Secure Configuration Policy outlines our commitment to the pseudonymisation and encryption of personal data.

Type of measure	Description"
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Wisetail ensures the ongoing confidentiality, integrity, availability, and resilience of processing systems and services through a comprehensive Business Continuity Plan, Disaster Recovery Plan, and Vendor Risk Management Procedures. These plans outline strategies based on Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). The company also conducts a Business Impact Analysis (BIA) to identify essential business units and processes and estimate the financial and operational impacts in a worst-case scenario. All vendors are evaluated for their potential risk to the business, and must meet defined minimum standards appropriate to their level of risk.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Wisetail has robust measures in place to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. These measures are outlined in our Disaster Recovery Plan and Business Continuity Plan, which are based on Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Our backup measures undergo regular testing to ensure alignment with our RTOs and RPOs.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Wisetail has established processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing. This is evidenced by our progress towards SOC 2 compliance, the operationalization of proving compliance, and the tasks completed for reviewing and remediating vulnerabilities. Our Information Security Committee and Security Program Committee provide oversight and conduct regular meetings to evaluate the performance and effectiveness of compliance controls. Additionally, our Threat and Vulnerability Management Policy includes regular vulnerability scans and annual external penetration tests.
Measures for user identification and authorisation	Wisetail employs measures for user identification and authorisation. We use unique user IDs and Multi-Factor Authentication (MFA) for additional security. Our Identity and Access Management Policy outlines stringent controls, including account creation approval, annual review of access rights, least privilege access, and timely modification of access rights upon role changes.
Measures for the protection of data during transmission	Wisetail employs several measures to protect data during transmission ensuring that customer data should not leave the protected environment.
Measures for the protection of data during storage	Wisetail has measures in place for the protection of data during storage. These include secure erasure of data from devices before disposal or reuse, encryption of data at rest in AWS, and encryption of removable media and backups. These practices are part of our Secure Disposal or Reuse and Encryption - Production Data at Rest controls.

Type of measure	Description"
Measures for ensuring physical security of locations at which personal data are processed	*Personal Data is processed through AWS and is not processed on prem for any Wisetail locations. However, where appropriate, Wisetail* has implemented measures which include restricted access to buildings and specific areas, monitored entry logs, and secure disposal of devices containing sensitive data. We also have a key management process
Measures for ensuring events logging	Wisetail ensures event logging through various measures as outlined in our Security Event and Incident Management Policy. We use AWS Tools for continuous threat detection and logging. Our logs include user IDs, system activities, dates, times, and details of relevant events, among other data. We also ensure the protection and integrity of log information. Our logs are produced, stored, protected, and analyzed to record events, generate evidence, and support investigations.
Measures for ensuring system configuration, including default configuration	Wisetail ensures system configuration, including default configuration, through a combination of change management and configuration management controls. We use standardized methods for handling changes, including system configurations, as outlined in our Change Control Procedures. Changes are managed through a structured process. We also use AWS Tools for managing system configurations and an MDM solution for workstation configuration. All changes and configurations follow our Secure Configuration Policy.
Measures for internal IT and IT security governance and management	Wisetail has established measures for internal IT and IT security governance and management. These measures are outlined in the Wisetail Risk Management Procedure, Risk Assessment and Treatment Policy, and the charters of the Wisetail Info Sec Committee and Security Program Committee. Wisetail's approach includes risk identification, analysis, evaluation, treatment, monitoring, and review. The roles and responsibilities of various entities such as the Senior Management/Executive Leadership, Director of Information Security, Cyber Security Analyst, and Information Security Committee are clearly defined. The company's risk treatment options include reducing, accepting, avoiding, or transferring risks.
Measures for certification/assurance of processes and products	Wisetail is actively working towards achieving SOC 2 compliance, We also have a system for reviewing and remediating vulnerabilities. Our Information Security Committee provides leadership and oversight in protecting our IT assets and ensures compliance with legal and regulatory requirements. We also have a Threat and Vulnerability Management Policy in place, which includes measures for certification and assurance of our processes and products.
Measures for ensuring data minimisation	Wisetail ensures data minimisation through various measures outlined in its Personnel Security and Awareness Training Policy and Identity and Access Management Policy. These include role-based access control, background checks, mandatory security awareness training, and a formal disciplinary process. Access to

Type of measure	Description"
	data is managed and minimized when employees leave the company, following the concept of 'least privilege'.
Measures for ensuring data quality	Wisetail ensures data quality through various measures. We use encryption for data stored in AWS. We have a robust backup system in place, with regular and systematic backups, and alerts for successful backup jobs. Our Disaster Recovery Plan and Business Continuity Policy outline procedures for rapid recovery and continuity of operations. We also have a Change Control Policy to manage changes that might affect data quality.
Measures for ensuring limited data retention	*Wisetail* has robust measures in place to ensure limited data retention. These include secure disposal or reuse of hardware, systematic secure wipe activities, and a comprehensive asset management policy. We also have a disaster recovery plan that includes key rotation procedures and a backup schedule. Our business continuity policy further supports these measures by outlining strategies for managing ICT continuity and disaster recovery.
Measures for ensuring accountability	*Wisetail* ensures accountability through several measures as outlined in our Personnel Security and Awareness Training Policy. These include job descriptions and candidate evaluations, background checks, terms and conditions of employment, segregation of duties, training and awareness, a disciplinary process, and annual performance evaluations. We have designated roles for information security, such as a Director of Information Security and a Cyber Security Analyst.
Measures for allowing data portability and ensuring erasure	*Wisetail* has measures in place for data portability and ensuring erasure. For data portability, we use removable media for storage of information and authorized cloud computing applications for sharing, storing, and transferring confidential or internal information, as outlined in our Asset Management Policy. We also have a comprehensive backup plan, including daily, hourly, monthly, and weekly backups stored in two different locations. For ensuring erasure, we have a secure disposal or reuse process for devices, which includes formatting and erasing all data from the device before it is disposed of or reused. This process is outlined in our Hardware Offboarding Process, Asana Hardware Offboarding Tasks, Secure Wipe Activities, Asset Disposal Standard, and Asset Management Policy.

EXHIBIT D

Additions to the Standard Contractual Clauses

The following capitalized term will have the meaning indicated below:

"UK Addendum" means the international data transfer addendum to the EU SCCs issued by the UK Information Commissioner under s. 119A of the Data Protection Act 2018, or such other addendum as may amend or replace the addendum from time to time.

"Completions" means

(i) in relation to the EU SCCs in relation to exports from the EEA:

a) the optional wording at Clauses 7 and 11 is deleted;

b) in Clause 8.9 of such SCCs, the following paragraph is added after subsection (d):

"*(e) Notwithstanding the above, any audit will be limited in scope and parameter to the systems processing the relevant personal data. Where audits include inspections, they shall be carried out with reasonable prior notice. The parties will mutually agree upon the scope, timing, duration, control and evidence requirements of the audit, provided that this requirement to agree will not permit the data importer to unreasonably delay performance of the audit.*

Any audit made pursuant to this Clause (i) shall be at the expense of the requesting data exporter, and such expenses shall include any reasonable related costs of the data importer, including compensation for the hours worked by the data importer's staff; (ii) may, if the data exporter seeks to retain an independent auditor, only be done byma party approved in advance by the data importer, which approval cannot be unreasonably withheld; and (iii) shall be subject to a non-disclosure agreement."

c) in Clause 9, Option 1 is deleted and the time period shall be not less than 30 days;

d) the applicable wording for Clause 13(a) of the EU SCCs (as determined by the instructions in square brackets in such SCCs) is retained and the two remaining alternatives are deleted;

e) in Clause 17 of the EU SCCs, Option 2 is deleted and Option 1 is completed with details of the laws of Ireland and in Clause 18(b) of the EU SCCs is completed with details of the courts of Ireland;

f) the parties set out in Annex 1 shall be completed with the names of the Customer as exporter and Wisetail as importer, the transfers shall be as described in Exhibit B and any other relevant exhibits for applicable additional Services under this DPA and the supervisory authority shall be the Irish supervisory authority; in Annex II the list of technical and organizational measures shall be the Technical and Organizational Measures and in Annex III the list of sub-processors shall be those set out in Exhibit A; and

g) in the event that the EU SCCs are replaced from those in force at the Effective Date, such completions shall be made to the revised SCCs as most closely replicate those set out above.

(ii) in relation to the EU SCCs in relation to exports from other jurisdictions besides the EEA the completions set out in (i)(a)-(g) above shall apply save that:

a) in Clause 17 of such EU SCC, the second sentence is replaced with the following: “The Parties agree that this shall be English law” save where another governing law of the EU SCCs is required as a mandatory requirement of the Data Protection Law of the relevant country, in which case Clause 17 shall be completed with details of the law which that Data Protection Law requires must be applied to such EU SCCs;

b) Clause 18(b) is replaced with the following “18(b) The Parties agree that those shall be the courts of England & Wales” save where another country, state or territory must have jurisdiction over the EU SCCs as a mandatory requirement of the Data Protection Law of the relevant country, in which case Clause 18(b) of such EU SCCs shall be completed with details of the country, state or territory which that Data Protection Law requires must have jurisdiction over the EU SCCs;

c) references in the EU SCC to “a third party located outside the European Union” are replaced by references to “a third party located outside the country or territory in which the data exporter is established”;

d) references in such EU SCC to “the Member State” are replaced by references to “the country or territory in which the data exporter is established”;

e) all references to the GDPR in such EU SCC are replaced by references to Data Protection Law of the relevant country and references to provisions or concepts of the GDPR are replaced by references to the provisions or concepts of such Data Protection Law most closely related to the relevant term as understood in the GDPR;

f) all references to Member States of the European Union or to the European Union are replaced by references to the country of establishment of the exporter;

g) save where required as mandatory requirement of the relevant Data Protection Law, all references in the EU SCC to (a) data subject rights or other third party beneficiary rights or (b) to obligations or liability towards data subjects or other third parties shall be deleted and ignored; and

h) to the extent that any of references to the EU SCCs referred to above under (i) to (viii) are replaced in any amended provisions or replacement or subsequently approved clauses or instrument after the Effective Date, the amendments provided above under (ii)(a)-(h) shall be adapted and/or completed if and to the extent appropriate to reflect the effect of the former as close as possible

(iii) in relation to SCCs in relation to exports from the UK the EU SCCs shall apply as amended by either (i) the Information Commissioner’s “UK Addendum to the EU Commission Standard Contractual Clauses” found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdfhttps://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf or (ii) such replacement addendum to the EU Standard Contractual Clauses as the Information Commissioner might issue from time to time (these addenda known as the “**UK SCC**”), with the following items completed (or in the case of (ii) those items as most closely approximate the following items):

a) to the extent not covered by the foregoing, the completions set out in (i)(a)-(g) above shall apply save that:

b) Table 1 shall be completed with the names of the Customer as exporter and Wisetail as importer;

c) in Table 2 the module of the EU SCCs selected shall be determined in accordance with the definition of SCCs set out below;

d) in Table 4 the “neither party” option shall be selected,

(iv) in relation to SCCs in relation to exports from Switzerland, the EU SCCs shall apply (incorporating the completions set out at (i)(a)-(g) above), as amended by either (a) the FDPIC’ decision guidance of 27 August 2021 found at https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1259254222 setting out amendments to be made to the EU SCCs in respect of transfers subject to the Swiss FADP or (b) such replacement decision of the FDPIC relating to amendments to be made to the EU SCCs from time to time (these amendments known as the “**Swiss SCCs**”);

(v) in relation to SCCs in relation to exports from any other country, the completions set out in (i)(a)-(g) above shall be made or such other Completions as most closely achieves the same outcome as those Completions.

In respect of any transfers of Personal Data that may occur in the course of the provision of the Service, Module 2 (Controller to Processor) terms, as provided below in Annex 1 to Exhibit D, shall apply to the extent Customer is a Controller of Customer Personal Data. The Module 3 (Processor to Processor) terms, as provided below in Annex 2 to Exhibit D, shall apply to the extent Customer is a Processor (or subprocessor) of Customer Personal Data. For both Module 2 and Module 3 of the Standard Contractual Clauses, the election of specific terms and/or addition of required information shall apply as follows:

(a) The applicable wording for Clause 13(a) of the Standard Contractual Clauses (as determined by the instructions in square brackets in the Standard Contractual Clauses) is retained and the two remaining alternatives are deleted;

(b) details of Subprocessors the data importer intends to engage as set out in Exhibit A and/or any other relevant exhibits for applicable additional Services, respectively, to this Agreement are the “agreed list” of Subprocessors referred to in Clause 9(a) of the Standard Contractual Clauses.