

## Data Processing Agreement

This Data Processing Addendum, including its Schedules, (“DPA”) forms part of the Master Services Subscription Agreement or other written or electronic agreement between Brightidea and Subscriber for the purchase of online services from Brightidea (identified either as “Services” or otherwise in the applicable agreement, and hereinafter defined as “Services”) (the “Agreement”) to reflect the Parties’ agreement with regard to the Processing of Personal Data.

Subscriber enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term “Subscriber” shall include Subscriber and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Subscriber pursuant to the Agreement, Brightidea may Process Personal Data on behalf of Subscriber and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

### HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, and 3.
2. This DPA has been pre-signed on behalf of Brightidea. Schedule 2, section 1 has been pre-signed by Brightidea Incorporated as the data importer. Schedule 3, Table 1 has been pre-signed by Brightidea Incorporated as the importer.
3. To complete this DPA, Subscriber must:
  - a. Complete the information in the signature box and sign on page 9.
  - b. Send the signed DPA to Brightidea by email to [data-privacy@brightidea.com](mailto:data-privacy@brightidea.com) indicating, if applicable, the Subscriber’s Company Name (as set out on the applicable Brightidea Order Form or invoice).

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by Brightidea of the validly completed DPA at this email address.

For the avoidance of doubt, signature of the DPA on page 9 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2 and Schedule 3. Where Subscriber wishes to separately execute the Standard Contractual Clauses and its Appendix, Subscriber should also complete the information as the data exporter and sign on page 13 (Schedule 2).

### HOW THIS DPA APPLIES

If the Subscriber entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Subscriber entity signing this DPA has executed an Order Form with Brightidea pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Form(s). For the purposes of this DPA, any reference to Order Form herein shall include “Ordering and Use of the Services” (as defined in the Agreement).

If the Subscriber entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Subscriber entity who is a party to the Agreement executes this DPA.

If the Subscriber entity signing the DPA is not a party to an Order Form nor an Agreement directly with Brightidea, but is instead a Subscriber indirectly via an authorized reseller of Brightidea services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

### DATA PROCESSING TERMS

#### 1. DEFINITIONS

**“Agreement”** means, as applicable, the Master Services Subscription Agreement, Order Form, SOW or similar commercial agreement by and between Brightidea and Subscriber with respect to the Service.

**“Authorized Affiliate”** means any of Subscriber’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Subscriber and Brightidea, but has not signed its own Agreement with Brightidea and is not the Subscriber as defined under this DPA.

**“Brightidea”** means the entity which is a party to this DPA, as specified in the section “HOW THIS DPA APPLIES” above being Brightidea Incorporated, a company incorporated in Delaware, US.

**“CCPA”** means the California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., and any binding regulations promulgated thereunder, in each case, as may be amended from time to time. This includes but it is not limited to the California Privacy Rights Act of 2020.

**“Controller”** means the entity which determines the purposes and means of the Processing of Personal Data.

**“Subscriber”** means the entity that executed the Agreement and/or Order Forms.

**“Subscriber Data”** means any data, information or other material provided, uploaded, or submitted by Subscriber to the Service in the course of using the Service.

**“Data Protection Laws and Regulations”** means all laws and regulations including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

**“Data Subject”** means the identified or identifiable person to whom Personal Data relates.

**“Europe”** means the European Union, the European Economic Area, Switzerland and the United Kingdom.

**“GDPR”** means 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 (General Data Protection Regulation). In respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2019 ("UK GDPR") and the Data Protection Act 2018 (together, "UK Data Protection Laws").

**“Personal Data”** means any information relating to (i) an identified or identifiable natural person and, (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 Regulations), where for each (i) or (ii), such data is Subscriber Data.

**“Processing”** or **“Process”** means any operation of 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.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

**“Public Authority”** means a government agency or law enforcement authority, including judicial authorities.

**"Security, Privacy and Architecture Documentation"** means the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Subscriber, as updated from time to time, and accessible via Brightidea's Security webpage at <https://brightidea.com/security>, or as otherwise made reasonably available by Brightidea.

**"Standard Contractual Clauses"** or **"SCCs"** means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 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, available at <https://eurlex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN> ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein ("UK SCCs") and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs") (in each case, as updated, amended or superseded from time to time).

**"Sub-processor"** means any Processor engaged by Brightidea.

## 2. PROCESSING OF PERSONAL DATA

- 2.1. **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Subscriber is a Controller or a Processor, Brightidea is a Processor and that Brightidea will engage Sub-processors pursuant to the requirements set forth in section 5 "Sub-processors" below.
- 2.2. **Subscriber's Processing of Personal data.** Subscriber shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirements to provide notice to Data Subjects of the use of Brightidea as Processor (including where the Subscriber is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Subscriber's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data. Subscriber specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.
- 2.3. **Brightidea's Processing of Personal Data.** Brightidea shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Subscriber's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in the use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Subscriber where such instructions are consistent with the terms of the Agreement.
- 2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by Brightidea is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Description of Processing/Transfer) to this DPA.

## 3. RIGHTS OF DATA SUBJECTS

Brightidea shall to the extent legally permitted, promptly notify Subscriber of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Brightidea shall not respond to a Data Subject Request itself, except that Subscriber authorizes Brightidea to redirect the Data Subject Request as necessary to allow Subscriber to respond directly. Taking into account the nature of the Processing, Brightidea shall assist Subscriber by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Subscriber's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request,

Brightidea shall, upon Subscriber's request, provide commercially reasonable efforts to assist Subscriber in responding to such Data Subject Request, to the extent Brightidea is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Subscriber shall be responsible for any costs arising from Brightidea's provision of such assistance.

#### 4. BRIGHTIDEA PERSONNEL

- 4.1. **Confidentiality.** Brightidea shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Brightidea shall ensure that such confidentiality obligations survives the termination of the personnel engagement.
- 4.2. **Reliability.** Brightidea shall take commercially reasonable steps to ensure the reliability of any Brightidea personnel engaged in the Processing of Personal Data.
- 4.3. **Limitation of Access.** Brightidea shall ensure that Brightidea's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.
- 4.4. **Data Protection Officer.** Brightidea has appointed a data protection officer. The appointed person may be reached at [data-privacy@brightidea.com](mailto:data-privacy@brightidea.com)

#### 5. SUB-PROCESSORS

- 5.1. **Appointment of Sub-processors.** Subscriber acknowledges and agrees that Brightidea may engage third-party Sub-processors in connection with the provision of the Services. Brightidea has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Subscriber Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- 5.2. **List of Current Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing, activities and countries of location, is listed under the Sub-processor documentation which can be found on Brightidea's Sub-processor support portal page at <https://support.brightidea.com/hc/en-us/articles/360001381768-Brightidea-Application-Sub-Processors>. Subscriber hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. The Sub-processor support portal webpage contains a mechanism to subscribe to notifications of new Sub-processors, and if Subscriber subscribes, Brightidea shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.
- 5.3. **Objection Right for New Sub-Processors.** Subscriber's may object to Brightidea's use of a new Sub-processor by notifying Brightidea promptly in writing within thirty (30) days of receipt of Brightidea's notice in accordance with the mechanism set out in section 5.2. If Subscriber objects to a new Sub-processor as permitted in the preceding sentence, Brightidea will use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Subscriber. If Brightidea is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Subscriber may terminate the applicable Agreement with respect only to those Services which cannot be provided by Brightidea without the use of the objected-to new Sub-processor by providing written notice to Brightidea. Brightidea will refund Subscriber any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Subscriber.
- 5.4. **Liability.** Brightidea shall be liable for the acts and omissions of its Sub-processors to the same extent Brightidea would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

#### 6. SECURITY

**6.1. Controls for the Protection of Subscriber Data.** Brightidea shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Subscriber Data), confidentiality and integrity of Subscriber data, as set forth in the Security, Privacy and Architecture Documentation. Brightidea regularly monitors compliance with these measures. Brightidea will not materially decrease the overall security of the Services during a subscription term.

**6.2. Audit.** Brightidea shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Subscriber information to demonstrate compliance with the obligations set out in this DPA as set forth in this section 6.2.

**6.2.1. Third-Party Certifications and Audits.** Brightidea has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Upon Subscriber's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Brightidea shall make available to Subscriber (or Subscriber's Third-Party Auditor - as defined below in section 6.2.4) information regarding Brightidea's compliance with the obligations set forth in this DPA in the form of a copy of Brightidea's then most recent third-party audits or certifications set forth in the Security, Privacy and Architecture Documentation. Such third-party audits or certifications may also be shared with Subscriber's competent supervisory authority on its request. Where Brightidea has obtained SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, Brightidea agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement. Upon request, Brightidea shall also provide a requesting Subscriber with a report and/or confirmation of Brightidea's audits of third party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Brightidea, to the extent such reports or evidence may be shared with Subscriber ("Third-party Sub-processor Audit Reports"). Subscriber acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Brightidea may require Subscriber to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

**6.2.2. On-Site Audit.** Subscriber may contact Brightidea to request an on-site audit of Brightidea's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Subscriber either itself or through a Third-Party Auditor (as defined below in section 6.2.4) selected by Subscriber when:

- (i) The information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;
- (ii) Subscriber has received a notice from Brightidea of a Subscriber Data Incident; or
- (iii) such an audit is required by Data Protection Laws and Regulations or by Subscriber's competent supervisory authority.

Any On-Site Audits will be limited to Subscriber Data Processing and storage facilities operated by Brightidea. Subscriber acknowledges that Brightidea operates a multi-tenant cloud environment. Accordingly, Brightidea shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Brightidea Subscribers' information.

**6.2.3. Reasonable Exercise of Rights.** An On-Site Audit shall be conducted by Subscriber or its Third-Party Auditor:

- (i) Acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Subscriber;
- (ii) Up to one time per year with at least three weeks advanced written notice. If an emergency justifies a shorter notice period, Brightidea will use good faith efforts to accommodate the On-Site Audit request; and
- (iii) During Brightidea's normal business hours, under reasonable duration and shall not unreasonably interfere with Brightidea's day-to-day operations.

Before any On-Site Audit commences, Subscriber and Brightidea shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Subscriber shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Brightidea.

**6.2.4. Third-Party Auditor.** A Third-Party Auditor means a third-party independent contractor that is not a competitor of Brightidea. An On-Site Audit can be conducted through a Third-Party Auditor if:

- (i) Prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Brightidea's proprietary information; and
- (ii) The costs of the Third-Party Auditor are at Subscriber's expense.

**6.2.5. Findings.** Subscriber must promptly provide Brightidea with information regarding any non-compliance discovered during the course of an On-Site Audit.

**6.3. Data Protection Impact Assessment.** Upon Subscriber's request, Brightidea shall provide Subscriber with reasonable cooperation and assistance needed to fulfill Subscriber's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Subscriber's use of the Services, to the extent Subscriber does not otherwise have access to the relevant information, and to the extent such information is available to Brightidea.

## 7. SUBSCRIBER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Brightidea maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and shall notify Subscriber without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Subscriber Data, including Personal Data, transmitted, stored or otherwise Processed by Brightidea or its Sub-processors of which Brightidea becomes aware (a "Subscriber Data Incident"). Brightidea shall make reasonable efforts to identify the cause of such Subscriber Data Incident and take such steps as Brightidea deems necessary and reasonable to remediate the cause of such a Subscriber Data Incident to the extent the remediation is within Brightidea's reasonable control. The obligation herein shall not apply to incidents that are caused by Subscriber or Subscriber's Users.

## 8. GOVERNMENT ACCESS REQUESTS

**8.1. Brightidea requirements.** In its role as a Processor, Brightidea shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Brightidea receives a legally binding request to access Personal Data from a Public Authority, Brightidea shall, unless otherwise legally prohibited, promptly notify Subscriber including a summary of the nature of the request. To the extent Brightidea is prohibited by law from providing such notification, Brightidea shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Brightidea to communicate as much information as possible, as soon as possible. Further, Brightidea shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Brightidea shall pursue possibilities of appeal. When challenging a request, Brightidea shall seek interim measures with a view to suspending the efforts of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Brightidea agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on any reasonable interpretation of the request. Brightidea shall promptly notify Subscriber if Brightidea becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Brightidea in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Brightidea to pursue action or inaction that could result in civil or criminal penalty for Brightidea such as contempt of court.

**8.2. Sub-processor requirements.** Brightidea shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

## 9. RETURN AND DELETION OF SUBSCRIBER DATA

Brightidea shall return Subscriber Data to Subscriber and, to the extent allowed by applicable law, delete Subscriber Data in accordance with the procedures and timeframes specified in the Agreement. Until Subscriber Data is deleted or returned, Brightidea shall continue to comply with this DPA and its Schedules.

## 10. AUTHORIZED AFFILIATES

**10.1. Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Subscriber enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Brightidea and each Authorized Affiliate subject to the provisions of the Agreement and this section 10 and section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. All access to and use of the Services by Authorized Affiliate must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Subscriber.

**10.2. Communication.** The Subscriber that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Brightidea under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

**10.3. Rights of Authorized Affiliates.** Where an Authorized Affiliate become party to this DPA with Brightidea, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

**10.3.1.** Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Brightidea directly by itself, the parties agree that (i) solely the Subscriber that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Subscriber that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set for, for example, in section 10.3.2, below).

**10.3.2.** The parties agree that the Subscriber that is the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Brightidea and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

## 11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates liabilities, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Brightidea, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Brightidea's and its Affiliates' total liability for all claims from Subscriber and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Subscriber and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or to any Authorized Affiliate this is a contractual party to any such DPA.

## 12. EUROPE SPECIFIC PROVISIONS

- 12.1. Definitions.** For the purpose of this sections 12 and Schedule 1 these terms shall be defined as follows:
- “**EU C-to-P Transfer Clauses**” means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor)
- “**EU P-to-P Transfer Clauses**” means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).
- 12.2. GDPR.** Brightidea will Process Personal Data in accordance with the GDPR requirements directly applicable to Brightidea’s provision of its Services.
- 12.3. Subscriber Instructions.** Brightidea shall inform Subscriber immediately (i) if, in its opinion, an instruction from Subscriber constitutes a breach of the GDPR and/or (ii) if Brightidea is unable to follow Subscriber’s instructions for the Processing of Personal Data.
- 12.4. Transfer mechanisms for data transfers.** If, in the performance of Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws and Regulations of Europe:
- **The EU C-to-P Transfer Clauses.** Where Subscriber and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Brightidea is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in section 2 of Schedule 1: and/or
  - **The EU P-to-P Transfer Clauses.** Where Subscriber and/or its Authorized Affiliates is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Brightidea is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of the EU P-to-P Transfer Clauses, subject to the additional terms in sections 2 and 3 of Schedule 1.
- 12.5. Impact of local laws.** As of the Effective Date, Brightidea has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Sub-processor documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Brightidea from fulfilling its obligations under this DPA. If Brightidea reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data (“Local Laws”) prevent it from fulfilling its obligations under this DPA, it shall promptly notify Subscriber. In such a case, Brightidea shall use reasonable efforts to make available to the affected Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber’s configuration or use of the Services to facilitate compliance with Local Laws without unreasonably burdening Subscriber. If Brightidea is unable to make available such change promptly, Subscriber may terminate the applicable Agreement(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Brightidea in accordance with Local Laws by providing written notice in accordance with the “Notices” section of the Agreement. Subscriber shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

### 13. CALIFORNIA CONSUMER PRIVACY ACT

This Section 13 shall apply from and after the CCPA Effective Date and shall apply in addition to, not in place of, any other requirements in this DPA.

- a. From and after the CCPA Effective Date, except as otherwise required by applicable law, Brightidea shall:
- Comply with its obligations under the CCPA and any rules or regulations promulgated thereunder;
  - Implement and maintain security procedures and practices consistent with industry-best standards appropriate to the nature of the Consumer Information to protect such Consumer Information from unauthorized access, destruction, use, modification, or disclosure;

- Not retain, use or disclose Consumer Information for any purpose outside the scope of the business relationship of the parties and other than for the specific purpose of performing services specified in the Agreement (including retaining, or disclosing the Consumer Information for a commercial purpose other than providing the services specified in the Agreement) or as otherwise permitted by the CCPA as applicable to service providers;
- Not collect or use Consumer Information except as necessary to perform the services specified in the Agreement;
- Not sell Consumer Information;
- Use industry standard efforts to assist Subscriber in Subscriber’s fulfillment of its obligation to respond to California residents’ requests to exercise rights with respect to their Consumer Information under the CCPA; and
- Use industry standard efforts to assist Subscriber to support Subscriber’s compliance with Subscriber’s obligations under the CCPA.

**14. ALTERNATIVE TRANSFER MECHANISMS**

To the extent Brightidea adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield) for the transfer of European Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Law and extends to the countries to which European Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer European Data (within the meaning of applicable European Data Protection Law), Brightidea may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of European Data.

**15. LEGAL EFFECT**

This DPA shall only become legally binding between Subscriber and Brightidea when the formalities steps set out in the section "HOW TO EXECUTE THIS DPA" above have been fully completed.

**List of Schedules**

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Description of Processing/Transfer

The parties’ authorized signatories have duly executed this DPA:

**BRIGHTIDEA INCORPORATED****SUBSCRIBER**Signature: *Vincent Carbone*

Signature: \_\_\_\_\_

Print Name: Vincent Carbone

Print Name: \_\_\_\_\_

Print Title: COO

Print Title: \_\_\_\_\_

Date: August 1, 2023

Date: \_\_\_\_\_

**SCHEDULE 1 – TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS****1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS**

For the purpose of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Subscriber is the data exporter and Brightidea is the data importer and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any reference to “Subscriber” in this Schedule, include such Authorized Affiliate. Where this section 1 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.

- 1.1. References to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.
- 1.2. Docking clause.** The option under clause 7 shall not apply.
- 1.3. Instructions.** This DPA and the Agreement are Subscriber’s complete and final documented instructions at the time of signature of the Agreement to Brightidea for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instruction by Subscriber to Process Personal Data are set out in section 1.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.
- 1.4. Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Brightidea to Subscriber only upon Subscriber’s written request.
- 1.5. Security of Processing.** For the purposes of clause 8.6(a), Subscriber is solely responsible for making an independent determination as to whether the technical and organizational measures set forth in the Security, Privacy and Architecture Documentation meet Subscriber’s requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Brightidea provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Subscriber Data Incident Management and Notification) of this DPA.
- 1.6. Audits of the SCCs.** The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.2 of this DPA.
- 1.7. General authorization for use of Sub-processors.** Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Brightidea has Subscriber’s general authorization to engage Sub-processors in accordance with section 5 of this DPA. Brightidea shall make available to Subscriber a current list of Sub-processors in accordance with section 5.2 of this DPA. Where Brightidea enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of Services, Subscriber hereby grants Brightidea authority to provide a general authorization on Controller’s behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.
- 1.8. Notification of New Sub-processors.** Pursuant to clause 9(a), Subscriber acknowledges and expressly agrees that Brightidea may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Brightidea shall inform Subscriber of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.
- 1.9. Complaints – Redress.** For the purposes of clause 11, and subject to section 3 of this DPA, Brightidea shall inform data subjects on its website of a contact point authorized to handle complaints. Brightidea shall inform Subscriber if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint of dispute to Subscriber. Brightidea shall not otherwise have any

obligation to handle the request (unless otherwise agreed with Subscriber) The option under clause 11 shall not apply.

- 1.10. Liability.** Brightidea's liability under clause 12(b) shall be limited to any damage caused by its Processing where Brightidea has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Subscriber, as specified in Article 82 GDPR.
- 1.11. Supervision.** Clause 13 shall apply as follows:
- 1.11.1.** Where Subscriber is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Subscriber with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- 1.11.2.** Where Subscriber is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.
- 1.11.3.** Where Subscriber is not established in an EU Member State, but falls within territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission Nationale de l'informatique et des Libertés (CNIL) - Paris, France shall act as competent supervisory authority.
- 1.11.4.** Where Subscriber is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as competent supervisory authority.
- 1.11.5.** Where Subscriber is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.
- 1.12. Notification of Government Access Requests.** For the purposes of clause 15(1)(a), Brightidea shall notify Subscriber (only) and not the Data Subject(s) in case of government access requests. Subscriber shall be solely responsible for promptly notifying the Data Subject(s) as necessary.
- 1.13. Governing Law.** The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of France; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.
- 1.14. Choice of forum and jurisdiction.** The courts under clause 18 shall be those designated in the Governing Law section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) France; or (ii) where the Agreement does not designate the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any disputes arising from Standard Contractual Clauses. From Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect to disputes.
- 1.15. Appendix.** The Appendix shall be completed as follows:
- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
  - The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
  - The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
  - The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses

**1.16. Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses.** In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland (“Swiss Data Protection Laws”), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom (“UK Data Protection Laws”) or Swiss Data protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

**1.17. Conflict.** The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

## **2. ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES**

For the purposes of the EU P-to-P Transfer Clauses (only), the Parties agree the following:

**2.1. Instructions and notifications.** For the purposes of clause 8.1(a), Subscriber hereby informs Brightidea that it acts as a Processor under the instructions of the relevant Controller in respect of Personal Data. Subscriber warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Brightidea for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Subscriber shall be solely responsible for forwarding any notifications received from Brightidea to the relevant Controller where appropriate.

**2.2. Security of Processing.** For the purpose of clause 8.6(c) and (d), Brightidea shall provide notification of a personal data breach concerning Personal Data Processed by Brightidea to Subscriber.

**2.3. Documentation and Compliance.** For the purpose of clause 8.9, all enquiries from the relevant Controller shall be provided to Brightidea by Subscriber. If Brightidea receives an enquiry directly from a Controller, it shall forward the enquiry to Subscriber and Subscriber shall be solely responsible for responding to any such enquiry from relevant Controller where appropriate.

**2.4. Data Subject Rights.** For the purpose of clause 10 and subject to section 3 of this DPA, Brightidea shall notify Subscriber about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Subscriber shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

**SCHEDULE 2 – DESCRIPTION OF PROCESSING/TRANSFER****1. LIST OF PARTIES**

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

Name: Subscriber and its Authorized Affiliates

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Role: For the purposes of the EU C-to-P Transfer Clauses Subscriber and/or its Authorized Affiliate is a Controller. For the purposes of the EU P-to-P Transfer Clauses Subscriber and/or its Authorized Affiliate is a Processor.

Data importer(s): Identity and contact details of the data importer(s), including any contact person with responsibility for data protection:

Name: Brightidea Incorporated

Address: 1040 Avenue of the Americas, Suite 18A, New York, NY 10018, USA

Contact person's name, position and contact details: Vincent Carbone, DPO, data-privacy@brightidea.com

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature: Vincent Carbone

Date: August 1, 2023

Role: Processor

**2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED**

Subscriber may submit Personal Data to the Services, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, Subscribers, business partners and vendors of Subscriber (who are natural persons)
- Employees or contract persons of Subscriber's prospects, Subscribers, business partners and vendors
- Employees, agents, advisors, freelancers of Subscribers (who are natural persons)
- Subscriber's Users authorized by Subscriber to use the Services

### 3. CATEGORIES OF PERSONAL DATA TRANSFERRED

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

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Localization data

### 4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

*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 specialized training) keeping a record of access to the data, restrictions for onward transfers or additional security measures:*

Not applicable with regard to the provision of Services.

### 5. FREQUENCY OF TRANSFER

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):*  
Continuous basis depending on the use of the Services by Subscriber.

### 6. NATURE OF THE PROCESSING

The nature of the Processing is the performance of the Services pursuant to the Agreement.

### 7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Brightidea will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Subscriber in its use of the Services.

### 8. DURATION OF PROCESSING

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:*

Subject to section 9 of the DPA, Brightidea will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

### 9. SUB-PROCESSOR TRANSFERS

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:*

As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to section 8 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed under the Sub-processor documentation which can be found on Brightidea's Sub-processor support portal page at <https://support.brightidea.com/hc/en-us/articles/360001381768-Brightidea-Application-Sub-Processors>

### 10. COMPETENT SUPERVISORY AUTHORITY

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative

pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Commission Nationale de l'informatique et des Libertés (CNIL) - Paris, France shall act as the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

## **11. TECHNICAL AND ORGANIZATIONAL MEASURES**

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific SCC Services purchased by data exporter, and accessible via <http://brightidea.com/security> or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the SCC Services during a subscription term. Data Subject Requests shall be handled in accordance with section 3 of the DPA.

SCHEDULE 3 – International Data Transfer Addendum (FOR UK DATA EXPORTERS) - UK IDTA

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective Date of the DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier): See details for Data Exporter in Schedule 2	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier): See details for Data Importer in Schedule 2
Key Contact	Full Name (optional): Job Title: Contact details including email: See contact details for Data Exporter in Schedule 2	Full Name (optional): Job Title: Contact details including email: See contact details for Data Importer in Schedule 2
Signature (if required for the purposes of Section 2)		<i>Vincent Carbone</i>

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: <b>Effective Date of the DPA</b>
------------------	---

		Reference (if any): <a href="#">See Model Clauses</a> Other identifier (if any): Or <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	N/A	N/A			
2	Yes	No	No	General	30 days	
3	No	N/A	N/A	N/A	N/A	
4	No	N/A	N/A			N/A

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Schedule 2

Annex 1B: Description of Transfer: See Schedule 2

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2

Annex III: List of Subprocessors (Modules 2 and 3 only): See Schedule 2

Table 4: Ending this Addendum when the Approved Addendum Changes

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR

As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

**Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

**Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
  - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;

c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - a. its direct costs of performing its obligations under the Addendum; and/or
  - b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.