THIS DATA PROCESSING ADDENDUM ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) **Hedra, Inc.,** a Delaware corporation ("**Hedra**"); and (2) the customer utilizing Hedra's Services ("**Customer**"), together the "**Parties**" and each a "**Party**".

HOW AND WHEN THIS DPA APPLIES

- This DPA is automatically incorporated into and forms a binding and effective part of the Agreement on and from the Addendum Effective Date.

- This DPA applies only if and to the extent Applicable Data Protection Laws govern Hedra's Processing of Customer Personal Data in performance of the services to be provided by Hedra under the Agreement (the "**Services**").

- This DPA does **not** apply to Hedra's Processing of Personal Data regarding Customer's Authorized Users or other representatives that Hedra may use for its own business/customer relationship administration purposes or its own marketing or service analytics, its own information and systems security purposes supporting the operation of the Services, nor its own legal, regulatory or compliance purposes.

1. **INTERPRETATION**

1.1 In this DPA (including the explanatory notes above) the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise. Capitalized terms used but not defined herein shall have the meanings provided in the Agreement:

(a) "**Addendum Effective Date**" means the effective date of the Agreement.

(b) "**Agreement**" means the agreement between the Parties that provides that this DPA will be incorporated therein by reference.

(c) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data under the Agreement, which are currently in effect and as they become effective, and as amended from time to time, including, as and where applicable, (i) Illinois' Biometric Information Privacy Act, the Texas Capture or Use of Biometric Identifiers Act, Tex. Bus. & Com. Code Ann. § 503.001, the Washington H.B. 1493, RCW 19.375, and any other laws relating to the privacy, security or Processing of Biometric Information (collectively, "**Biometric Privacy Laws**"); (ii) the GDPR, and (iii) the CCPA.

(d) "**Biometric Information**" means "biometric identifiers," "biometric information," "biometric data" or any similar term defined in Applicable Data Protection Laws. Biometric Information shall include, without limitation, a retina or iris scan, fingerprint, voiceprint, and scan of face or hand geometry and any information, regardless of how it is captured, converted, stored, or shared, based on such data.

(e) "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any binding regulations promulgated thereunder.

(f) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(g) "**Customer Personal Data**" means any Personal Data Processed by Hedra or its Sub-Processor on behalf of Customer to perform the Services under the Agreement (including, for the avoidance of doubt, any such Personal Data comprised within Content, Input and Output).

(h) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(i) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Customer Personal Data and the Processing thereof.

(j) "**EEA**" means the European Economic Area.

(k) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law (as amended from time to time) ("**UK GDPR**").

(l) "**Personal Data**" means (i) Biometric Information, and (ii) "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws.

(m) "**Personal Data Breach**" means a breach of Hedra's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data in Hedra's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(n) "**Personnel**" means a person's employees, agents, consultants, contractors or other staff.

(o) "**Process**" and inflections thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(p) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

(q) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Customer Personal Data to any person located in: (i) in the context of the EU GDPR, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "**EEA Restricted Transfer**"); and (ii) in the context of the UK GDPR, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(r) "**SCCs**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(s) "**Sensitive Personal Data**" means data classified as "sensitive personal data", "sensitive data," "special category data," "sensitive personal information," or similar term defined in Applicable Data Protection Laws.

(t) "**Sub-Processor**" means any third party appointed by or on behalf of Hedra to Process Customer Personal Data.

(u) "**Supervisory Authority**": (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office.

(v) "**UK Transfer Addendum**" means the template Addendum B.1.0 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 of the UK Mandatory Clauses included in Part 2 thereof (the "**UK Mandatory Clauses**").

2. APPLICATION OF THIS DATA PROCESSING ADDENDUM

2.1 The front-end of this DPA applies generally to Hedra's Processing of Customer Personal Data under the Agreement.

2.2 Annex 2 (European Annex) applies only if and to the extent Hedra's Processing of Customer Personal Data under the Agreement is subject to the GDPR.

2.3 Annex 3 (California Annex) applies only if and to the extent Hedra's Processing of Customer Personal Data under the Agreement is subject to the CCPA.

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 The Parties acknowledge and agree that the details of Hedra's Processing of Customer Personal Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 (Data Processing Details) to the DPA.

3.2 Hedra shall not Process Customer Personal Data other than: (a) on Customer's instructions; or (b) as required by applicable laws provided that, in such circumstances, Hedra shall inform Customer in advance of the relevant legal requirement requiring such Processing if and to the extent Hedra is: (i) required to do so by Applicable Data Protection Laws; and (ii) permitted to do so in the circumstances. Customer instructs Hedra to Process Customer Personal Data to provide the Services to Customer and in accordance with the Agreement. The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on Hedra only pursuant to any written amendment to this DPA signed by both Parties. Where required by Applicable Data Protection Laws, if Hedra receives an instruction from Customer that, in its reasonable opinion, infringes Applicable Data Protection Laws, Hedra shall notify Customer.

3.3 The Parties acknowledge that Hedra's Processing of Customer Personal Data authorized by Customer's instructions stated in this DPA is integral to the Services and the business relationship between the Parties. Access to Personal Data does not form part of the consideration exchanged between the Parties in respect of the Agreement or any other business dealings.

4. HEDRA PERSONNEL

Hedra shall take commercially reasonable steps designed to ascertain the reliability of any Hedra Personnel who Process Customer Personal Data and shall enter into written confidentiality agreements with all Hedra Personnel who Process Customer Personal Data that are not subject to professional or statutory obligations of confidentiality.

5. **SECURITY**

5.1 Hedra shall implement and maintain technical and organisational measures in relation to Customer Personal Data designed to protect Customer Personal Data against Personal Data Breaches as described in Annex 4 (Security Measures) (the "**Security Measures**").

5.2 Hedra may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Customer Personal Data.

6. **DATA SUBJECT RIGHTS**

6.1 Hedra, taking into account the nature of the Processing of Customer Personal Data, shall provide Customer with such assistance as may be reasonably necessary and technically feasible to assist Customer in fulfilling its obligations to respond to Data Subject Requests. If Hedra receives a Data Subject Request, Customer will be responsible for responding to any such request.

6.2 Hedra shall: (a) promptly notify Customer if it receives a Data Subject Request; and (b) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Customer, except as required by Applicable Data Protection Laws.

7. **PERSONAL DATA BREACH**

7.1 Hedra shall notify Customer without undue delay upon Hedra's confirmation of a Personal Data Breach affecting Customer Personal Data. Hedra shall provide Customer with information (insofar as such information is within Hedra's possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Hedra) to allow Customer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. Hedra's notification of or response to a Personal Data Breach shall not be construed as Hedra's acknowledgement of any fault or liability with respect to the Personal Data Breach.

7.2 Customer is solely responsible for complying with applicable laws (including notification laws), and fulfilling any third-party notification obligations, related to any Personal Data Breaches.

7.3 If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, any other governmental authority, any Data Subject(s), the public or others under Applicable Data Protection Laws or otherwise, to the extent such notice directly or indirectly refers to or identifies Hedra, where permitted by applicable laws, Customer agrees to: (a) notify Hedra in advance; and (b) in good faith, consult with Hedra and consider any clarifications or corrections Hedra may reasonably recommend or request to any such notification, which: (i) relate to Hedra's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

8. **SUB-PROCESSING**

8.1 Customer generally authorises Hedra to appoint Sub-Processors in accordance with this Section 8. Information about Hedra's Sub-Processors, including their functions and locations is as shown in Annex 5 (Authorised Sub-Processors) (the "**Sub-Processor List**"). Without limitation, Customer authorises Hedra engagement of the Sub-Processors listed on the Sub-Processor List as of the Addendum Effective Date.

8.2 Hedra shall give Customer prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor by providing Customer with an updated copy of the Sub-Processor List (including via a 'mailshot' or similar bulk distribution mechanism sent to Customer's contact point set out in Annex 1 (Data Processing Details)).

If, within fourteen (14) days of receipt of that notice, Customer notifies Hedra in writing of any objections (on reasonable grounds) to the proposed appointment: (a) Hedra shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and (b) where: (i) such a change cannot be made within fourteen (14) days from Hedra's receipt of Customer's notice; (ii) no commercially reasonable change is available; and/or (iii) Customer declines to bear the cost of the proposed change, then Customer may terminate the Agreement by written notice to Hedra as its sole and exclusive remedy.

8.3 If Customer does not object to Hedra's appointment of a Sub-Processor during the objection period referred to in Section 8.2, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

8.4 With respect to each Sub-Processor, Hedra shall maintain a written contract between Hedra and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Customer Personal Data as those set out in this DPA (including the Security Measures). Hedra shall remain liable for any breach of this DPA caused by a Sub-Processor.

9. AUDITS

9.1 Hedra shall make available to Customer on request, such information as Hedra (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

9.2 Subject to Sections 9.3 to 5, in the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Hedra pursuant to Section 9.1 is not sufficient in the circumstances to demonstrate Hedra's compliance with this DPA, Hedra shall, at Customer's sole expense, allow for and contribute to audits, including on-premise inspections, by Customer or an auditor mandated by Customer (provided such auditor agrees to a non-disclosure agreement reasonably acceptable to Hedra) in relation to the Processing of Customer Personal Data by Hedra.

9.3 Customer shall give Hedra reasonable notice of any audit or inspection to be conducted under Section 9.2 (which shall in no event be less than fourteen (14) days' notice) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Hedra's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Hedra's other customers or the availability of Hedra's services to such other customers).

9.4 If the controls or measures to be assessed in the requested audit are assessed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request ("**Audit Report**") and Hedra has confirmed in writing that there have been no known material changes in the controls audited and covered by such Audit Report(s), Customer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures. Hedra shall provide copies of any such Audit Reports to Customer upon request; provided that they shall constitute the confidential information of Hedra, which Customer shall use only for the purposes of confirming compliance with the requirements of this DPA or meeting Customer's obligations under Applicable Data Protection Laws.

9.5 Hedra need not give access to its premises for the purposes of such an audit or inspection: (a) where an Audit Report is accepted in lieu of such controls or measures in accordance with Section 4; (b) to any individual unless they produce reasonable evidence of their identity; (c) to any auditor whom Hedra has not approved in advance (acting reasonably); (d) to any individual who has not entered into a non-

disclosure agreement with Hedra on terms acceptable to Hedra; (e) outside normal business hours at those premises; or (f) on more than one occasion in any calendar year during the term of the Agreement, except for any audits or inspections which Customer is required to carry out under the GDPR or by a Supervisory Authority. Nothing in this DPA shall require Hedra to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers. Nothing in this Section 9 shall be construed to obligate Hedra to breach any duty of confidentiality.

10. RETURN AND DELETION

10.1 Upon expiration or earlier termination of the Agreement, or upon Customer's written request, Hedra shall return and/or delete all Customer Personal Data in Hedra's care, custody or control in accordance with Customer's reasonable instructions. To the extent that deletion of any Customer Personal Data contained in any back-ups' maintained by or on behalf of Hedra is not technically feasible within the timeframe set out in Customer's instructions, Hedra shall (a) securely delete such Customer Personal Data in accordance with any relevant scheduled back-up deletion routines (e.g., those contained within Hedra's relevant business continuity and disaster recovery procedures); and (b) pending such deletion, put such Customer Personal Data beyond use.

10.2 Notwithstanding the foregoing, Hedra may retain Customer Personal Data where required by applicable laws, provided that Hedra shall (a) maintain the confidentiality of all such Customer Personal Data and (b) Process the Customer Personal Data only as necessary for the purpose(s) and duration specified in the applicable law requiring such retention.

11. CUSTOMER'S RESPONSIBILITIES

11.1 Customer shall:

(a) ensure that there is, and will be throughout the term of the Agreement, a valid legal basis for Customer's Processing of Customer Personal Data and for the Processing by Hedra of Customer Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable));

(b) comply (and is solely responsible for complying) with all Applicable Data Protection Laws in connection with its Processing of Customer Personal Data, and Customer represents and warrants that Hedra's Processing of Customer Personal Data as contemplated by and in accordance with the Agreement and this DPA shall not violate any Applicable Data Protection Laws; and

(c) (i) present all Data Subjects with all required notices and statements; and (ii) obtain all required consents, in each case (i) and (ii) relating to the collection of Customer Personal Data, sharing of Customer Personal Data with Hedra, and Processing by Hedra of Customer Personal Data as contemplated by the Agreement and this DPA, including under and in compliance with all Applicable Data Protection Laws. For the avoidance of doubt, such notices, statements and consents shall include, without limitation, all notices to, and all consents obtained from and written releases executed by, Data Subjects in relation to the Processing of their Biometric Information required under Biometric Privacy Laws, and all consents to process Sensitive Personal Data as are required under Applicable Data Protection Laws. Customer shall maintain

auditable records of all such Data Subject consents and shall make such records available to Hedra upon request.

11.2 The Parties acknowledge and agree that Biometric Information may be created or Processed in connection with the Services and that Hedra's Processing of Biometric Information in connection with the Services is solely for the purpose of providing the Services to, and on behalf of, Customer. Customer is solely responsible for complying with all applicable data retention and destruction requirements, including, without limitation, as applicable to Biometric Information under applicable Biometric Privacy Laws.

11.3 Customer agrees that the Services, the Security Measures, and Hedra's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Customer Personal Data. Other than as expressly agreed in Annex 1, Customer shall not provide or otherwise make available to Hedra any Customer Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding a Data Subject's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) passwords to any online accounts; (e) credentials to any financial accounts; (f) tax return data; (g) any payment card information subject to the Payment Card Industry Data Security Standard; (h) Personal Data of children under 16 years of age; or (i) any other information that falls within any special categories of personal data (as set out in Article 9(1) of the GDPR) and/or data relating to criminal convictions and offences or related security measures (together, "**Restricted Data**").

12. LIABILITY

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA and the SCCs (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the Agreement; **provided that**, nothing in this Section 12 will affect any person's liability to Data Subjects under relevant third-party beneficiary provisions of the SCCs (if and as they apply).

13. VARIATION

Hedra may on notice vary this DPA to the extent that (acting reasonably) it considers necessary to address the requirements of Applicable Data Protection Laws from time to time, including by varying or replacing the SCCs in the manner described in Paragraph 2.5 of Annex 2 (European Annex) and/or to reflect any relevant changes in the Services and its Processing of Personal Data as part thereof.

14. INCORPORATION AND PRECEDENCE

14.1 In the event of any conflict or inconsistency between: (a) this DPA and the Agreement, this DPA shall prevail; or (b) any SCCs entered into pursuant to Paragraph 2 of Annex 2 (European Annex) and this DPA and/or the Agreement, the SCCs shall prevail in respect of the Restricted Transfer to which they apply.

Annex 1

Data Processing Details

Note: this Annex 1 (Data Processing Details) to the DPA includes certain details of the Processing of Customer Personal Data as required: (a) by certain Applicable Data Protection Laws; and (b) to populate the Appendix to the SCCs in the manner described in Paragraph 2.2(d) of Annex 2 (European Annex).

HEDRA / 'DATA IMPORTER' DETAILS

Name:	Hedra, Inc.
Address:	As set out in the pre-amble to the DPA
Contact Details for Data Protection:	Customer's primary point of contact with Hedra; or any other email notified by Hedra for the purpose of providing it with data protection-related communications or alerts.
Hedra Activities:	Hedra offers a social media and video content generation platform for users to create and export AI generated videos and video components
Role:	Processor

CUSTOMER / 'DATA EXPORTER' DETAILS

Name:	Provided by Customer
Address:	Provided by Customer
Contact Details for Data Protection:	Hedra's primary point of contact with Customer; or any other email notified by Customer for the purpose of providing it with data protection-related communications or alerts.
Customer Activities:	Customer's activities relevant to this DPA are the receipt of the Services as part of its ongoing business operations under and in accordance with the Agreement (including the access and use of the Solution via the APIs in the manner permitted under the Agreement).
Role:	Controller

DETAILS OF PROCESSING

Categories of Data Subjects:	Any Data Subjects whose Personal Data is comprised within data submitted to the Services by or on behalf of Customer (including by Authorized Users) under the Agreement, which will be as determined by Customer in its sole discretion through its use of the Services in accordance with the Agreement – but may include: • Customer's personnel. • Individuals whose data is contained in any databases or other files submitted to the Services or otherwise Processed or made available to the Services. • Suppliers, service providers, vendors and other providers of goods

	or services. Each category includes current, past and prospective Data Subjects.
Categories of Personal Data:	Any Personal Data comprised within data submitted to the Services by or on behalf of Customer (including by End Users) under the Agreement, which will be Customer's responsibility and under Customer's control, through use of the Services – but may include: • **Contact details** – for example home and/or business address, email address, telephone details and other contact information such as social media identifiers/handles. • **Biometric details** – for example, facial geometry scans, voiceprints and other Biometric Information. • **Images** – for example, images or graphics that include any Data Subject's image and likeness or other information relating to them. • **Video** – for example, video recordings that include any Data Subject's image and likeness or other information relating to them. • **Other user-generated content** – for example, Personal Data included in text Inputs.
Special Categories of Data under the GDPR, and associated additional restrictions/safeguards:	Special category data under the GDPR: None Additional safeguards for special category data: N/A
Frequency of transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the Agreement.
Purpose of the Processing:	Customer Personal Data will be processed pursuant to Section 3.2 of the DPA.
Duration of Processing / Retention Period:	For the period determined in accordance with the Agreement and DPA, including Section 10 of the DPA.
Transfers to (sub-)processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with Section 8 of the DPA).

Annex 2

European Annex

1. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**

Hedra, taking into account the nature of the Processing and the information available to Hedra, shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by Hedra.

2. **RESTRICTED TRANSFERS**

2.1 Entry into Transfer Mechanisms

(a) *EEA Restricted Transfers.* To the extent that any Processing of Customer Personal Data under this DPA involves an EEA Restricted Transfer from Customer to Hedra, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be (i) populated in accordance with Section 2.2 of this Annex 2 (European Annex); and (ii) entered into by the Parties and incorporated by reference into this DPA.

(b) *UK Restricted Transfers.* To the extent that any Processing of Customer Personal Data under this DPA involves a UK Restricted Transfer from Customer to Hedra, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (i) varied to address the requirements of the UK GDPR in accordance with the UK Transfer Addendum and populated in accordance with Sections 2.2 and 2.3 of this Annex 2 (European Annex); and (ii) entered into by the Parties and incorporated by reference into this DPA.

2.2 Population of SCCs

(a) *Signature of SCCs*. Where the SCCs apply in accordance with Paragraph 2.1(a) and/or Paragraph 2.1(b) of this Annex 2 (European Annex), each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

(b) *Modules of SCCs*. As and where relevant: Module Two of the SCCs applies to any EEA Restricted Transfer involving Processing of Personal Data in respect of which Customer is a controller in its own right; and/or Module Three of the SCCs applies to any EEA Restricted Transfer involving Processing of Personal Data in respect of which Customer is a processor.

(c) *Population of body of SCCs*. As and where applicable to the relevant Module and the Clauses thereof: (i) in Clause 7: the 'Docking Clause' is not used; (ii) in Clause 9: 'Option 2: General Written Authorisation' applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Section 8.2 of the DPA; (iii) in Clause 11: the optional language is not used; (iv) in Clause 13: all square brackets are removed and all text therein is retained; (v) in Clause 17: 'OPTION 1' applies, and the Parties agree that the SCCs shall be governed by the law of Ireland in relation to any EEA Restricted Transfer; and (vi) in Clause 18(b): the Parties agree that any dispute arising from the SCCs in relation to any EEA Restricted Transfer shall be resolved by the courts of Ireland.

(d) *Population of Appendix to SCCs*. Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 (Data Processing Details) to the DPA, with: Customer being 'data exporter'; and Hedra being 'data importer', and Part C to that Annex I is populated with: the competent Supervisory Authority shall be determined as follows: (i) where Customer is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Customer is established; and (ii) where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EEA Representative under Article 27 of the GDPR: the competent Supervisory Authority shall be the Supervisory Authority of the EU Member State in which Customer's EEA Representative relevant to the Processing hereunder is based (from time-to-time), which Customer shall notify to Hedra in writing. Annex II shall be populated with reference to the information contained in or determined by Section 2.3 of the DPA (including the Security Measures).

2.3 UK Restricted Transfers

(a) *UK Transfer Addendum*. Where relevant in accordance with Section 2.1(b) of this Annex 2 (European Annex), the SCCs apply to any UK Restricted Transfers as varied by the UK Transfer Addendum in the following manner: (i) 'Part 1 to the UK Transfer Addendum': (A) the Parties agree: Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Data Processing Details) to the DPA and Section 2.2 of this Annex 2 (European Annex); and (B) Table 4 to the UK Transfer Addendum is completed with 'Data Importer' only; and (ii) 'Part 2 to the UK Transfer Addendum': the Parties agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum and that the SCCs shall apply to any UK Restricted Transfers as varied in accordance with those Mandatory Clauses.

(b) *Interpretation*. As permitted by section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner determined by 2.3(a) of this Annex 2 (European Annex); **provided that** the Parties further agree that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in section 3 of the UK Mandatory Clauses). In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in this Section 2.3 of this Annex 2 (European Annex).

2.4 Operational Clarifications

(a) When complying with its transparency obligations under Clause 8.3 of the SCCs, Customer agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect Hedra's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

(b) Where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Hedra to notify any third-party controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer.

(c) For the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

(d) The terms and conditions of Section 8 of the DPA apply in relation to Hedra's appointment and use of Sub-Processors under the SCCs. Any approval by Customer of Hedra's appointment of a Sub-Processor that is given expressly or deemed given pursuant to that Section 8 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the SCCs.

(e) The audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in Section 9 of the DPA.

(f) Certification of deletion of Personal Data as described in Clauses 8.5 and 16(d) of the SCCs shall be provided only upon Customer's written request.

(g) In respect of any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject or further Controller (where applicable) – on specific written request; accompanied by suitable supporting evidence of the relevant request), Hedra shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with relevant provisions of this DPA in respect of the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

2.5 *Adoption of new transfer mechanism*

Hedra may on notice vary this DPA and replace the relevant SCCs with: (a) any new form of the relevant SCCs or any replacement therefor prepared and populated accordingly (e.g., standard data protection clauses adopted by the European Commission for use specifically in respect of transfers to data importers subject to Article 3(2) of the EU GDPR); or (b) another transfer mechanism, other than the SCCs, that enables the lawful transfer of Customer Personal Data by Customer to Hedra under this DPA in compliance with Chapter V of the GDPR.

Annex 3 California Annex

1. In this Annex 3, the terms "**business**," "**business purpose**," "**commercial purpose**," "**consumer**," "**sell,**" "**share**," and "**service provider**" shall have the respective meanings given thereto in the CCPA; and "**personal information**" shall mean Customer Personal Data that constitutes "personal information" as defined in and that is subject to the CCPA.

2. The business purposes and services for which Hedra is Processing personal information are for Hedra to provide the Services to and on behalf of Customer and as otherwise set forth in the Agreement, as described in more detail in Annex 1 (Data Processing Details) to the DPA.

3. It is the Parties' intent that with respect to any personal information, Hedra is a service provider. Hedra (a) acknowledges that personal information is disclosed by Customer only for limited and specific purposes described in the Agreement; (b) shall comply with applicable obligations under the CCPA and shall provide the same level of privacy protection to personal information as is required by the CCPA; (c) agrees that Customer has the right to take reasonable and appropriate steps under and subject to the Compliance Review section of the DPA to help ensure that Hedra's use of personal information is consistent with Customer's obligations under the CCPA; (d) shall notify Customer in writing of any determination made by Hedra that it can no longer meet its obligations under the CCPA; and (e) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

4. Hedra shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the business purposes specified in the Agreement, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purpose specified in the Agreement, or as otherwise permitted by CCPA; (c) retain, use or disclose the personal information outside of the direct business relationship between Hedra and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Hedra's own interaction with any consumer to whom such personal information pertains.

5. Hedra shall implement reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, Customer, in accordance with Section 5 (Security Measures) of the DPA.

6. When Hedra engages any Sub-Processor, Hedra shall notify Customer of such Sub-Processor engagements in accordance with Section 8 (Sub-Processing) of the DPA and that such notice shall satisfy Hedra's obligation under the CPRA to give notice of such engagements.

7. Hedra agrees that Customer may conduct audits, in accordance with Section 9 of the DPA, to help ensure that Hedra's use of personal information is consistent with Hedra's obligations under the CCPA.

8. The Parties acknowledge that Hedra's retention, use and disclosure of personal information authorized by Customer's instructions documented in the Agreement and DPA are integral to Hedra's provision of the Services and the business relationship between the Parties.

Annex 4 Security Measures

As from the Addendum Effective Date, Hedra will implement and maintain the Security Measures as set out in this Annex 4.

1. Organisational management and staff responsible for the development, implementation and maintenance of Hedra's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Hedra's organisation, monitoring and maintaining compliance with Hedra's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Customer Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of production resources relevant to the Services is maintained by the relevant Sub-Processor(s) (and their vendors) engaged from time-to-time by Hedra to host those resources. Hedra takes steps to ensure that such Sub-Processors provide appropriate assurances and certifications that evidence such physical and environmental security – including security of data centre, server room facilities and other areas containing Customer Personal Data designed to:

   (a) protect information assets from unauthorised physical access,

   (b) manage, monitor and log movement into and out of Sub-Processor facilities, and

   (c) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Hedra's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Hedra's technology and information assets.

10. Incident management procedures designed to allow Hedra to investigate, respond to, mitigate and notify of events related to Hedra's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

Hedra may freely update or modify these Security Measures from time to time **provided that** such updates and modifications do not materially decrease the overall security of the Services and/or relevant Customer Personal Data.

Annex 5 Authorised Sub-Processors

Sub-Processor	Function	Location
Amazon Web Services	Hosting services provider for all core functionalities of any platform-based elements of the Services	United States
Together AI	Hosting services provider for all core functionalities of any platform-based elements of the Services	United States
ElevenLabs	Voice provider for generating realistic, human-like audio outputs	United States
Cartesia	Voice provider for generating realistic, human-like audio outputs	United States
Oracle	Cloud infrastructure and database management provider; supporting data storage, hosting, and processing.	United States
OpenAI	Provider for content moderation and filtering capabilities.	United States
Hive AI	Provider for content moderation and filtering capabilities.	United States
Fal	Provider for text-to-image generation for character creation.	United States
Black Forest Labs	Provider for text-to-image generation for character creation.	Germany
Anthropic	Provider for agentic AI capabilities.	United States