Immersive Labs Data Processing Addendum – Controller to Processor

This Addendum is made between:

(1) **Immersive Labs** (as such term is defined in section 1 below)

and

(2) **Customer**,

(each a "**Party**", and together the "**Parties**").

Whereas:

(A) This Data Processing Addendum, including the Contractual Safeguards where applicable ("**DPA**"), is entered into between the Customer entity and the Immersive Labs entity identified in the applicable master agreement(s) governing the Customer's use of Immersive Labs' products and services (the "**Main Agreement**").

(B) This DPA is incorporated by reference into the Main Agreement. All capitalized terms used in this DPA but not defined will have the meaning set forth in the Main Agreement.

(C) To the extent of any conflict or inconsistency between this DPA, any previously executed data processing addendum, and the remaining terms of the Main Agreement, this DPA will govern.

(D) This DPA sets out the terms that apply when Personal Data is processed by Immersive Labs on the Customer's behalf under the Main Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with Data Protection Legislation and respects the rights of individuals whose personal data is processed under the Main Agreement.

IT IS AGREED THAT:

1. Definitions

In this DPA, the following expressions shall have the following meanings unless the context otherwise requires:

"**Affiliate(s)**" means any entity controlling, controlled by, or under common control of the subject entity. For the purposes of this definition, "control" (including with correlative meanings, the terms "controlled by" and "under common control with"), as used with respect to the subject entity, means the possession, directly or indirectly, of the power to direct or exercise a controlling influence on the management or policies of such entity, whether through the ownership of voting securities, by contract or otherwise;

"**Authorized Affiliate(s)**" means any of the Customer's Affiliate(s) which (a) is subject to Data Protection Legislation, and (b) receives or is otherwise using products and/or Services pursuant to the Main Agreement;

"**CCPA**" means the California Consumer Privacy Act of 2018;

"**Contractual Safeguards**" means (i) where the GDPR applies, the standard contractual clauses annexed to the EU Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council (the "**EU SCCs**"); and (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (the "**UK Addendum"**);

"**Customer**" means the Customer and/or any Authorized Affiliate that is a party to the Main Agreement and that controls Personal Data processed under this DPA;

The terms "**controller**", "**data subject**", "**personal data**" (notwithstanding the capitalized definition provided further below), "**process**", "**processing**", "**processor**" will have the same meanings as defined by Data Protection Legislation. Other relevant terms such as "**business**", "**business purpose**", "**consumer**", "**personal information**", "**sale**" (including the terms "**sell**", "**selling**", "**sold**", and other variations thereof), "service **provider**", and "**third party**" have the meanings given to those terms under the CCPA;

"**Data Protection Legislation**" means applicable national, federal, state, provincial, and local laws and regulations governing the use and disclosure of personal information, including the CCPA, the GDPR, the UK GDPR and the Data Protection Act 2018.

"**EEA**" means the European Economic Area;

"**EU**" means the European Union;

"**GDPR**" means Regulation (EU) 2016/679 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 (Data Protection Directive);

"**Immersive Labs**" means Immersive Labs Limited, Immersive Labs Corporation, Immersive Labs GmbH or any other Immersive Labs entity that is a party to the Main Agreement and that processes personal data as defined under relevant Data Protection Legislation;

"**Personal Data**" means personal data Immersive Labs processes on behalf of the controller as a processor during the course of providing products and Services to the Customer under this DPA;

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

"**Restricted Transfer(s)**" means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA or an (onward) transfer from a country outside of the EEA within the same country or to another country outside of the EEA, which are not subject to an adequacy decision under Article 45 GDPR by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country or an (onward) transfer from a country outside of the United Kingdom within the same country or to another country outside of the United Kingdom, which are not subject to adequacy regulations adopted pursuant to Article 45(1) UK GDPR in conjunction with Section 17A of the United Kingdom Data Protection Act 2018;

"**Services**" means the services to be provided under the Main Agreement;

"**Subprocessor(s)**" means any processor engaged by Immersive Labs who agrees to receive Personal Data intended for processing on behalf of the Customer in connection with the provision of Immersive Labs products and/or Services;

"**UK**" means the United Kingdom of Great Britain and Northern Ireland;

"**UK GDPR**" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 c. 16;

Any reference to "**writing**" or "**written**" includes email, unless expressly indicated to the contrary.

2. Scope and Application of this DPA to Customer and Immersive Labs

2.1 The parties acknowledge that to the extent Immersive Labs processes Personal Data on the Customer's behalf when performing its obligations under the Main Agreement, the Customer is the controller and Immersive Labs is the processor for the purposes of Data Protection Legislation.

2.2 The subject matter, nature, purpose and type of Personal Data and the categories of data subjects affected are set out in Annex I of the Appendix to this DPA.

2.3 This DPA should be read in conjunction with Immersive Labs' Acceptable Use Policy, Privacy Notice and Cookie Notice available at www.immersivelabs.com/legal as updated from time to time.

2.4 The parties acknowledge and agree that to the extent Immersive Labs processes Personal Data in connection with the Main Agreement to: (i) monitor, prevent and detect fraud, and to prevent harm to the Customer, Immersive Labs and Immersive Labs Affiliates, and to third parties; (ii) comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Immersive Labs is subject; (iii) analyse, develop and improve Immersive Labs products, services and solutions; or (iv) provide the Immersive Labs products, services and/or solutions to Immersive Labs users, Immersive Labs is acting as a data controller with respect to the processing of such Personal Data it receives from or through the Customer.

3. Data Processing

To the extent Immersive Labs processes personal data on behalf of Customer as a processor, Immersive Labs agrees to process the Personal Data in accordance with Data Protection Legislation and the terms and conditions set out in this DPA. In particular, Immersive Labs agrees to:

3.1 act only on written instructions and directions from the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by laws to which Immersive Labs is subject; in such a case, Immersive Labs shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. For the purposes of this clause 3.1, the Customer's instructions shall include those contained in this DPA, the Main Agreement, and those instructions and directions received from the Customer from time to time. Immersive Labs shall process Personal Data in accordance with this DPA (including Schedule 1), and to the extent reasonably necessary for the performance of the Main Agreement or this DPA;

3.2 only disclose the Personal Data to any government or third party where necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or binding order of a government body, Immersive Labs will give the Customer notice of any legal requirement or order referred to in this clause 3.2;

3.3 notify the Customer promptly where Immersive Labs believes that compliance with any instructions by the Customer would result in a violation of Data Protection Legislation;

3.4 implement and maintain appropriate technical and organizational measures to adequately protect the Personal Data processed on behalf of the Customer against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, as required under Data Protection Legislation.

3.5 ensure that any Immersive Labs' personnel entrusted with the processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality no less restrictive than those confidentiality obligations included in the Main Agreement;

3.6 provide reasonable assistance to the Customer if requested, to assist with the Customer's compliance with its obligations under Data Protection Legislation (including Articles 32 to 36 of the UK GDPR and the EU GDPR as applicable), and/or in responding to any request from a data subject;

3.7 take all appropriate measures pursuant to Article 32 of the UK GDPR and/or the EU GDPR (as applicable), having regard to the state of technological development and the cost of implementing any measures;

3.8 maintain a record of its processing activities and provide cooperation and information to the Customer as is necessary for the Customer to demonstrate compliance with its obligations pursuant to Data Protection Legislation;

3.9 permit audits conducted by the Customer (or any authorised third party on the basis that such third party is not a competitor of Immersive Labs (as determined by Immersive Labs)) no more than once in any 12-month period provided that:

3.9.1 the Customer gives Immersive Labs at least 30 business days' notice of the audit (such notice shall include details of any third party which the Customer wishes to conduct the audit) and the scope, nature, timing and duration of the audit is agreed between the parties in writing prior to the audit;

3.9.2 the Customer or such authorised party enter into a confidentiality agreement (to Immersive Labs' satisfaction) with Immersive Labs; and

3.9.3 Customer will provide Immersive Labs any audit reports generated in connection with any audit under this clause, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory requirements and/or confirming compliance with the requirements of the Main Agreement and this DPA. The audit report(s) and any information obtained by Customer under this clause are Immersive Labs' Confidential Information under the terms of the Main Agreement.

3.10 Immersive Labs will promptly (in any event within 48 hours) notify the Customer on becoming aware of:

3.10.1 a Personal Data Breach; and/or

3.10.2 any request received directly from a data subject.

3.11 The Customer agrees that where there is an attempt to gain access to Customer Data (as defined in the Main Agreement) or the infrastructure and networks that provide the Platform (as defined in the Main Agreement) (including pings, denial of service attacks, attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, packet sniffing or other unauthorised access to traffic data) which does not result in a Personal Data Breach Immersive Labs have no obligation to notify the Customer under the Main Agreement or this DPA.

3.12 **Appointment of Subprocessors**

3.12.1 The Customer gives Immersive Labs general authorization to engage those Subprocessors listed at www.immersivelabs.com/legal as updated from time to time, in accordance with clause 3.12.2 ("**Subprocessor List**").

3.12.2 Immersive Labs shall update the Subprocessor List whenever it adds a Subprocessor or makes any changes to the hosting location of an existing Subprocessor. Customer shall be entitled to receive prior notice of changes to the Subprocessor List by subscribing to www.immersivelabs.com/legal. To exercise its right to object to Immersive Labs' use of a new Subprocessor, the Customer shall notify Immersive Labs promptly in writing within ten (10) business days after receipt of Immersive Labs' notice. In the event the Customer objects to a proposed new Subprocessor, and that objection is reasonable (including where such objection relates to bona fide concerns regarding the proposed sub-processors' data security), Immersive Labs will work with the Customer (whereby both parties shall act reasonably) to consider how the Platform (as defined in the Main Agreement) may be delivered to the Customer in a way which remedies the original objection of the Customer. If the parties cannot agree such an alternative delivery of the Platform within 30 days of the Customer's objection, the Customer may terminate any affected part of the Main Agreement by giving written notice to Immersive Labs. If the Customer does not object, the Customer shall be deemed to have accepted the change to the Subprocessor List.

3.12.3 Any processing by a Subprocessor shall be pursuant to a written agreement that is substantially similar to this DPA.

3.12.4 Immersive Labs shall remain fully responsible for its Subprocessors' acts, omissions and defaults.

3.13 **Data Transfers**

3.13.1 The Customer authorises Immersive Labs and its Subprocessors to make Restricted Transfers of Personal Data to comply with the Customer's instructions under this DPA and perform the obligations under the Main Agreement, provided such Restricted Transfer complies with Data Protection Legislation.

3.13.2 The Parties agree that when the transfer of Personal Data from the Customer (as "Data Exporter") to Immersive Labs (as "Data Importer") is a Restricted Transfer and Data Protection Legislation requires that appropriate safeguards are put in place, the Parties will be subject to the EU SCCs and UK Addendum as applicable and attached to this DPA.

4. Obligations of Customer

4.1 The Customer shall:

4.1.1 ensure that the Customer's instructions always comply with all applicable Data Protection Legislation;

4.1.2 (and hereby does) warrant and represent that it has a lawful basis for sending, storing and receiving the Personal Data and that the Customer is entitled to transfer the Personal Data to Immersive Labs so that Immersive Labs, its group, Affiliates and Subprocessors may process them in accordance with this Agreement;

4.1.3 (and hereby does) acknowledge Immersive Labs reliance on this clause.

4.2 The Customer Data (as defined in the Main Agreement) may be shared between the Customer's Authorised Users (as defined in the Main Agreement) for the purposes of leader-boards and team games or otherwise as directed by the Customer.

5. Duration; Termination; Return or Deletion of Personal Data

5.1 This DPA will become effective when the Parties' Main Agreement enters into effect into which this DPA has been incorporated.

5.2 This DPA will terminate automatically upon the later of (i) termination or expiry of the Main Agreement; (ii) termination of processing of the Personal Data by Immersive Labs. On termination of this DPA, Immersive Labs shall delete, all Personal Data processed on behalf of the Customer unless the Customer requests the return of the Personal Data or to the extent that Data Protection Legislation requires storage of such Personal Data.

6. Liability

6.1 The limits and exclusions on a Party's liability set out in the Main Agreement shall apply to that Party's liability under this DPA (and the Contractual Safeguards), *mutatis mutandis*, provided that the foregoing shall not operate to limit or exclude a Party's liability to a data subject under the Contractual Safeguards.

7. GENERAL

7.1 In the case of conflict between the terms of the Main Agreement and the terms of this DPA, the terms of the DPA shall take precedence. In the event of any conflict or inconsistency between the above clauses of this DPA and the Contractual Safeguards referenced therein, the latter shall prevail.

7.2 Amendments or additions to this DPA and its Appendix must be made in writing and agreed between the Parties to be effective. This shall also apply to amendments of this written form requirement. For the purposes of this clause, the written form requirement includes signature by commercially acceptable electronic means (e.g., DocuSign) but does not include email.

7.3 Should any provision of this DPA be or become invalid, this shall not affect the validity of the remaining terms.

7.4 Any of Immersive Labs' or the Customer's obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this DPA.

7.6 **CCPA.** If and to the extent that Immersive Labs processes any personal information relating to an end user of the Customer, an Authorized Affiliate, or customer of the Customer within the scope of the CCPA, Immersive Labs acts as a Service Provider as defined in the CCPA. The Customer or Authorized Affiliate respectively discloses end user personal information to Immersive Labs, if any, solely for: (i) a valid business purpose; and (ii) to permit Immersive Labs to provide the Services under the Main Agreement. Immersive Labs will not (i) sell the personal information, (ii) retain, use, or disclose the personal information for a commercial purpose other than providing the Services; or (iii) retain, use, or disclose the personal information outside of the provision of the Services to the Customer or Authorized Affiliate respectively pursuant to the Main Agreement.

7.5 This Addendum shall be governed by the same law that is governing the Main Agreement between the Parties, except for the Contractual Safeguards, which shall be governed by the law applicable pursuant to the applicable Contractual Safeguards.

SCHEDULE 1

- **Subject matter of the processing:** Such processing operations necessary for performance of the Vendor’s obligations under the DPA.
- **Duration of the processing**: Unless the Personal Data is otherwise deleted by the Customer, the Term of the Main Agreement.
- **Location of processing:** United Kingdom, United States of America and Europe and as otherwise set out in this DPA or the Main Agreement.
- **Nature and purpose of the processing:** Provisioning user access to the Platform (by way of bulk upload or SSO), providing in-platform or custom reporting, and providing professional services.
- **Type of Personal Data:** First name, last name, email address, IP address, display picture, user ID.
- **Categories of Data Subjects:** The Customer’s employees, workers, contractors, consultants, directors, and Authorised Users (as defined in the Main Agreement).

A detailed description of the uses, purposes of the processing of personal data (as defined in the Main Agreement) is set out in Immersive Labs privacy notice at www.immersivelabs.com/legal.

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES MODULE TWO

CONTROLLERS AND PROCESSORS

SECTION I

Clause 1 – Purpose and Scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 – Effect and Invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 – Third-party beneficiaries

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Docking Clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 – Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10 – Data Subject Rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 – Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 – Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability

Clause 13 – Supervision

(a) 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, as indicated in Annex I.C, 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, as indicated in Annex I.C, 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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 – Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects 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. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

(f) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(g) The Parties agree that those shall be the courts of Ireland.

(h) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(i) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I to the Standard Contractual Clauses

A. List of Parties

Controller(s) (Data Exporter)	**Details/Descriptions**
Name:	The Customer as set out in the Main Agreement
Address:	Address as listed in the Main Agreement
Contact person's name, position and contact details:	Contact information as listed in the Main Agreement
Activities relevant to the data transferred under these Clauses:	Activities relevant are described in Section B below
Signature and date:	See relevant Order Form
Role (controller/processor):	Controller

Processor(s) (Data Importer)	**Details/Descriptions**
Name:	Immersive Labs
Address:	Address as listed in the Main Agreement
Contact person's name, position and contact details:	Contact information as listed in the Main Agreement
Activities relevant to the data transferred under these Clauses:	Activities relevant are described in Section B below
Signature and date:	See relevant Order Form
Role (controller/processor):	Processor

B. Description of the Transfer

Categories of data subjects whose personal data is processed
The categories of data subjects to whom the personal data relates are:

Customer's and its Affiliates' employees, workers, contractors.

Categories of personal data processed
The categories of personal data to be processed are:

Full name, business email address, username, User ID, IP address

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. *N/A*

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

The provision of the products or services to the Customer in accordance with the Main Agreement.

Purpose(s) of the data transfer and further processing

To provide the products or services to the Customer as described in the Main Agreement.

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

For as long as necessary to provide the products or services as described in the Main Agreement, as legally or contractually required, or upon receipt of the Customer's written request for deletion.

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

Details of Immersive Labs' sub-processors, the subject matter, and nature of their processing is set out at https://www.immersivelabs.com/company/legal/.

The relevant sub-processors processing will continue for the duration of the Main Agreement (as defined in the main body of the DPA).

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13

The Data Protection Commission Ireland

Annex II to the Standard Contractual Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Immersive Labs, as a Data Importer, will implement and maintain technical and organizational security measures appropriate to safeguard data against unauthorized destruction, alteration, loss, disclosure or access as set out in this annex II.

1. Information Security Policies

Immersive Labs implements security rules in the form of mandatory policies, standards, and procedures. These policies, standards and procedures cover:

- technical and organizational measures, rules and norms to address the appropriate level of security of personal data;
- employee functions and obligations;
- procedures for reporting, managing and responding to information security incidents; and
- business continuity planning.

These rules are kept up to date and revised appropriately when relevant changes are made to an information system that uses or houses personal data, or to how that system is organised.

The security policies, standards and procedures include (without limitation) provisions relating to:

- preventing unauthorized persons from gaining access to personal data processing systems (physical access control);
- preventing personal data processing systems being used without authorisation (logical access control);
- ensuring that persons entitled to use a personal data processing system gain access only to such personal data as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorization (data access control);
- ensuring that personal data is protected against accidental destruction or loss (availability control);
- ensuring that personal data collected for different purposes can be processed separately (separation control);
- notification of identified data breaches;
- system access controls;
- user privilege controls;
- software development and change controls;
- communications security;
- administrative security;
- access to facilities and premises housing IT hardware and software; and
- anti-virus protection.

2. Physical Security

All data importer sites at which an information system that uses or houses personal data is located have commercially reasonable security systems. The data importer or their vendor/supplier appropriately restricts access to such personal data.

Physical access control has been implemented for all data centres through AWS. Unauthorized access is prohibited through 24x7 monitoring and access limitation.

3. Organisational Security

When electronic media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of the information, including personal data, stored on them. When media are to leave the premises at which the files are located in connection with maintenance operations, procedures have been implemented to prevent unauthorized retrieval of the information stored on them.

Immersive Labs has implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

All personal data security incidents are managed in accordance with appropriate incident response procedures relating to personal data.

All personal data transmitted by Immersive Labs is encrypted while in transit and at rest.

4. Network Security

Immersive Labs maintains network security using commercially available equipment and industry standard IT security tools and techniques, including intrusion detection and prevention systems, access control lists and routing protocols.

5. Application Development and Security

Immersive Labs has established a Secure Software Development Lifecycle (**SDLC**) for the development of its software services, which follows industry best practice and incorporates guidelines for developers in respect of application security, code hygiene and release, peer review, quality assurance and testing.

6. Access Control

Only authorised employees can grant, modify or revoke access to an information system that uses or houses personal data.

User administration procedures define user roles and their privileges, how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms.

Access rights are implemented adhering to the “least privilege” approach.

Immersive Labs implements physical and electronic security controls for the creation and protection of passwords and other authentication methods

7. Virus and Malware Controls

Immersive Labs installs and maintains up to date anti-virus and malware protection software on the system.

8. Personnel

Immersive Labs implements a security awareness program to train personnel about their information security obligations. This program includes training about data classification obligations; physical security controls; security practices and threats, and security incident reporting.

The data importer has clearly defined roles and responsibilities for the employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

Immersive Labs employees strictly follow established security policies and procedures. Disciplinary process will be applied if employees are found to have committed a security breach.

9. Business Continuity

Immersive Labs implements and maintains appropriate disaster recovery and business resumption plans. Immersive Labs reviews both business continuity plan and risk assessment regularly. Business continuity plans are being tested and updated regularly to ensure that they are up to date and effective.

10. Risk Management

Immersive Labs has established a risk management framework to identify, record and manage risks associated with the collection, storage and processing of customer personal data. Identified risks are regularly reviewed and treatment plans are implemented to mitigate risks deemed to be unacceptable.

11. Vendor Management

Immersive Labs has implemented a vendor management programme to ensure that third party risk to customer personal data and to the provision of services is minimized.

12. Compliance and Certification

Immersive Labs has achieved the following certifications:

- ISO/IEC 27001:2013
- Cyber Essentials

Certificates may be found on the Immersive Labs website here: https://www.immersivelabs.com/company/security-docs/.

Annex III to the Standard Contractual Clauses

Details of Immersive Labs’ sub-processors, the subject matter, and nature of their processing is set out at https://www.immersivelabs.com/company/legal/.

UK Addendum to the Standard Contractual Clauses

Part 2: Mandatory Clauses

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		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer, recipient of the Services Trading name (if different): Main address (if a company registered address): Address as listed in the Main Agreement Official registration number (if any) (company number or similar identifier): Company number as listed in the Main Agreement	Full legal name: Immersive Labs, provider of the Services Trading name (if different): Main address (if a company registered address): Address as listed in the Main Agreement Official registration number (if any) (company number or similar identifier): Company number as listed in the Main Agreement
Key Contact	Contact information as listed in the Main Agreement	Contact information as listed in the Main Agreement
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ **The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** Date: [Insert] Reference (if any): Other identifier (if any): Or ☒ 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	N/A					
2	Yes		N/A	General Auth	14 days	
3	N/A					
4	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 Annex 1A of the Standard Contractual Clauses above
Annex 1B: Description of Transfer: See Annex 1B of the Standard Contractual Clauses above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the Standard Contractual Clauses above
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III of the Standard Contractual Clauses above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: **X Importer** ☐ Exporter ☐ 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.