DATA PROCESSING ADDENDUM

(Revision March 2024)

This Data Processing Addendum, including its applicable Schedules, ("**DPA**") forms part of the Hexagon Aura Reality Software License Agreement or other written or electronic agreement incorporating this DPA by reference (the "**Agreement**") between Hexagon Aura Reality AG ("**HAR**") and Customer for the purchase of HAR products and services (hereinafter defined as "**Services**").

In the course of providing the Services to Customer pursuant to the Agreement, HAR may Process Personal Data on behalf of Customer and this DPA sets forth their obligations with respect to the Processing.

All capitalized terms used in this DPA but not defined herein will have the meaning set forth in the Agreement. In the event of any conflict or inconsistency between the terms of the DPA and Agreement, the DPA terms shall prevail.

1. DEFINITIONS

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Agreement**" shall have the meaning ascribed to it in in the Preamble.

1.3. "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.4. "**Customer**" means the entity that executed the Agreement.

1.5. "**Data Protection Laws and Regulations**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to those of the European Union (GDPR), the European Economic Area and their member states, Switzerland, and the United Kingdom.

1.6. "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.7. "**Data Subject Request**" shall have the meaning ascribed to it in Section 3.1.

1.8. "**Data Transfer Addendum**" means the cross-border data transfer mechanism outlined in ***Schedule 1*** that fulfills the requirements of certain Data Protection Laws and Regulations.

1.9. "**DPA**" shall have the meaning ascribed to it in the Preamble.

1.10. "**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 Personal Data.

1.11. "**HAR**" shall have the meaning ascribed to it in the Preamble.

1.12. "**Party**" means either HAR or t Customer individually, and "**Parties**" refers to both HAR and Customer collectively.

1.13. "**Personal Data**" means any information relating to an identified or identifiable natural person Processed by HAR under this DPA on behalf of Customer.

1.14. "**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.

1.15. "**Processing**" or "**Process**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16. "**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

1.17. "**Public Authority**" means a competent government agency or law enforcement authority under Data Protection Laws and Regulations, including judicial authorities.

1.18. "**Restricted Transfer**" means any transfer of Personal Data to countries outside of the originating jurisdiction, which does not ensure an adequate level of protection, or which is not authorized by Data Protection Laws and Regulations of the originating jurisdiction. This includes any transfer that requires specific safeguards to be in place to protect the privacy and fundamental rights of Data Subjects, such as binding corporate rules, standard contractual clauses approved by Public Authority, explicit consent from the Data Subject, approval by Public Authority, or other transfer mechanisms deemed acceptable under Data Protection Laws and Regulations.

1.19. "**Sensitive Data**" refers to Personal Data that receives elevated protection under applicable Data Protection Laws and Regulations. This may include, but is not limited to, Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the Processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, and children's Personal Data.

1.20. "**Services**" shall have the meaning ascribed to it in the Preamble.

1.21. "**Sub-processor**" means any subsequent data processor engaged by the Processor to perform some or all of the data Processing tasks on behalf of the Controller.

2. PROCESSING OF PERSONAL DATA

2.1. Customer as Controller or Processor shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of HAR as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject to the extent applicable under Data Protection Laws and Regulations.

2.2. HAR as Processor shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the purposes of the Agreement.

2.3. The subject-matter of Processing of Personal Data by HAR is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the

Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in ***Schedule 2, Annex II*** to this DPA.

2.4. HAR shall inform Customer immediately: (i) if, in its opinion, an instruction from Customer constitutes a breach of the Data Protection Laws and Regulations; and/or (ii) if HAR is unable to follow Customer's instructions for the Processing of Personal Data.

3. RIGHTS OF DATA SUBJECTS

3.1. HAR shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". HAR shall not respond to a Data Subject Request itself, except that Customer authorizes HAR to redirect the Data Subject Request as necessary to allow Customer to respond directly.

3.2. Taking into account the nature of the Processing, HAR shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, HAR shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent HAR is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from HAR's provision of such assistance.

4. CONFIDENTIALITY AND LIMITATION OF ACCESS

HAR shall grant access to Personal Data to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. HAR shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. SUB-PROCESSORS

5.1. Customer acknowledges and agrees that: (a) HAR's Affiliates may be retained as Sub-processors; and (b) HAR and HAR's Affiliates respectively may engage third-party Sub-processors to provide the Services, provided that third-party Sub-processors adhere to adequate privacy and security protocols. HAR or an HAR Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. HAR has Customer's general authorization for the engagement of Sub-processors from an agreed list. The agreed list of Sub-processors engaged in Processing Personal Data for the performance of Service, including a description of their Processing activities and countries of location, are listed on ***Schedule 2, Annex IV***. HAR shall specifically inform Customer in writing of any intended

changes of that list through the addition or replacement of Sub-processors at least thirty (30) days in advance. HAR shall provide Customer with the information necessary to enable Customer to exercise the right to object.

5.3. Customer may object to HAR's use of a new Sub-processor by notifying HAR promptly in writing within thirty (30) days of receipt of HAR's notice in accordance with the mechanism set out in Section 5.2.

5.4. If Customer objects to a new Sub-processor as permitted in the preceding sentence, HAR will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If HAR is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the Agreement with respect only to those Services which cannot be provided by HAR without the use of the objected-to new Sub-processor by providing written notice to HAR. HAR will refund Customer any prepaid fees covering the remainder of the term of such Services following the effective date of termination, without imposing a penalty for such termination on Customer.

5.5. HAR shall be liable for the acts and omissions of its Sub-processors to the same extent HAR would be liable as if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY, DOCUMENTATION, AUDIT AND DATA PROTECTION IMPACT ASSESSMENT

6.1. HAR shall at least implement the technical and organizational measures specified in ***Schedule 2, Annex III*** to ensure the security of Personal Data. This includes protecting Personal Data against a breach of security leading to a 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 purposes of Processing and the risks involved for the Data Subjects.

6.2. HAR shall grant access to Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. HAR shall ensure that persons authorized to Process Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.3. The Parties shall be able to demonstrate compliance with the DPA. HAR shall deal promptly and adequately with inquiries from Customer about the Processing of Personal Data in accordance with the terms of the DPA. HAR shall make available to Customer all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from the Data Protection Laws and Regulations.

6.4. At Customer's request, HAR shall also permit and contribute to audits of the Processing activities covered by this DPA, up to one time per year with at least three (3) weeks' advance written notice or if there are indications of non-compliance. If an emergency justifies a shorter notice period, HAR will use good faith efforts to accommodate the audit request. Customer acknowledges that HAR operates a multi-tenant cloud environment. The audits shall be conducted during HAR's normal business hours, under reasonable duration and shall not unreasonably interfere with HAR's day-to-day operations. Before any audit commences, Customer and HAR shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of HAR. HAR shall have the right to reasonably adapt the scope of any audit to avoid or mitigate risks with respect to, and including, service levels, availability, and

confidentiality of other HAR customers' information. Customer must promptly provide HAR with information regarding any non-compliance discovered during the course of an audit.

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

7. NOTIFICATION OF PERSONAL DATA BREACH

7.1. In the event of a Personal Data Breach, HAR shall cooperate with and assist Customer for Customer to comply with its obligations under Data Protection Laws and Regulations, taking into account the nature of Processing and the information available to HAR.

7.2. In the event of a Personal Data Breach concerning Personal Data Processed by Customer, HAR shall assist Customer:

7.2.1. in notifying the Personal Data Breach to Public Authority, where applicable;

7.2.2. in obtaining the information which, pursuant to Data Protection Laws and Regulations, shall be stated in Customer's notification, such as:

(a) the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
(b) the likely consequences of the Personal Data Breach;
(c) the measures taken or proposed to be taken by Customer to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.2.3. in complying, pursuant to Data Protection Laws and Regulations, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, where applicable.

7.3. In the event of a Personal Data Breach concerning Personal Data Processed by HAR, HAR shall notify Customer without undue delay after HAR having become aware of the breach. Such notification shall contain, at least:

7.3.1. a description of the nature of Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned);

7.3.2. the details of a contact point where more information concerning Personal Data Breach can be obtained; and

7.3.3. its likely consequences and the measures taken or proposed to be taken to address Personal Data Breach, including to mitigate its possible adverse effects.

7.4. Where, and insofar as, it is not possible to provide all this 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.

8. INTERNATIONAL TRANSFERS

8.1. The use of Services, whether through on-premise or cloud installations, may involve the transfer of Personal Data to the EEA, Switzerland and India.

8.2. Where Processing Personal Data involves Restricted Transfer and Data Transfer Addendum is deemed an appropriate mechanism under Data Protection Laws and Regulations to safeguard such Restricted Transfer, the Parties agree to incorporate Data Transfer Addendum in this DPA.

8.3. Where Processing Personal Data involves Restricted Transfer and Data Transfer Addendum is not deemed an appropriate mechanism under Data Protection Laws and Regulations to safeguard such Restricted Transfer, the Parties shall ensure compliance with Data Protection Laws and Regulations pertaining to Restricted Transfer, as applicable to them. This might include, but is not limited to, employing anonymization techniques where feasible, obtaining necessary consents from Data Subjects and completing any required registrations with or permission from Public Authority.

9. SENSITIVE DATA

If the Customer uses Services to Process Sensitive Data, the Customer is responsible for complying with Data Protection Laws and Regulations applicable to Processing Sensitive Data. This might include, but is not limited to, obtaining consent from Data Subjects. HAR will Process Sensitive Data following the Customer's documented instructions and protect that Sensitive Data in accordance with the technical and organizational measures specified in ***Schedule 2, Annex III***.

10. LIMITATION OF LIABILITY

Each Party's and all of its Affiliates' total liability for all claims in the aggregate, arising out of or related to this DPA, and its applicable Schedules, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and DPA together.

11. NON-COMPLIANCE AND TERMINATION

11.1. Without prejudice to any provisions of Data Protection Laws and Regulations, in the event that HAR is in breach of its obligations under this DPA, Customer may instruct HAR to suspend the Processing of Personal Data until the latter complies with the DPA or the Agreement is terminated. HAR shall promptly inform Customer in case it is unable to comply with this DPA, for whatever reason. Customer shall be entitled to terminate the DPA insofar as it concerns Processing of Personal Data in accordance with these Clauses if:

(a) the Processing of Personal Data by HAR has been suspended by Customer pursuant to point 11.1 and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;
(b) HAR is in substantial or persistent breach of this DPA or its obligations under Data Protection Laws and Regulations;
(c) HAR fails to comply with a binding decision of Public Authority regarding its obligations pursuant to this DPA or to Data Protection Laws and Regulations.

11.2. HAR shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data under this DPA where, after having informed Customer that its instructions infringe applicable Data Protection Laws and Regulations in accordance with Section 2.4., Customer insists on compliance with the instructions.

11.3. Following termination of Agreement, HAR shall, at the choice of Customer, delete all Personal Data Processed on behalf of Customer and certify to Customer that it has done so, or return all Personal Data to Customer and delete existing copies unless Data Protection Laws and Regulations requires storage of Personal Data. Until Personal Data is deleted or returned, HAR shall continue to ensure compliance with this DPA.

List of Schedules

SCHEDULE 1: DATA TRANSFER ADDENDUM

Introduction

This Data Transfer Addendum forms part of the DPA, which in turn is part of the Hexagon Aura Reality Software License Agreement or another written or electronic agreement that incorporates the DPA by reference (the "**Agreement**") between Hexagon Aura Reality AG ("**HAR**") and Customer for the purchase of HAR products and services (hereinafter defined as "**Services**").

All capitalized terms used in this Data Transfer Addendum but not defined herein, in documents incorporated by reference, or through links, will have the meanings set forth in the Agreement and the DPA. In the event of any conflict or inconsistency among the terms of the DPA, the Agreement, and this Data Transfer Addendum, the terms of the latter shall prevail.

This Data Transfer Addendum consists of four (4) parts and Appendix:

- **Part 1** shall apply for Restricted Transfers by controllers-exporters and processors-exporters subject to the GDPR.
- **Part 2** shall apply for Restricted Transfers by controllers-exporters and processors-exporters subject to the UK Data Protection Laws.
- **Part 3** shall apply for Restricted Transfers by controllers-exporters and processors-exporters subject to the the Swiss Federal Data Protection Act (FADP).
- **Part 4** shall apply for Restricted Transfers by controllers-exporters and processors-exporters subject to Data Protection Laws and Regulations other than GDPR, the UK Data Protection Laws, and FADP.
- **Appendix** shall apply to all Restricted Transfers as directed/modified by each Part.

Part 1: EEA Restricted Transfer Mechanism

For Restricted Transfers initiated by controllers-exporters and processors-exporters subject to the GDPR, the Modules 2 and 3 of the EU Standard Contractual Clauses for transfers shall apply, modified as follows:

(a) Clause 7 (Docking Clause) shall not apply.

(b) For Clause 9a (Use of sub-processors) Option 2 (General Written Authorisation) is selected to read as follows:

> *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 30 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.*

(c) The optional provision in Clause 11a (Redress) shall not apply.

(d) Clause 13(a) is modified to read as follows:

Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of

Article 27(1) of Regulation (EU) 2016/679 is established, shall act as 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, shall act as competent supervisory authority.

The data exporter shall, upon the data importer's request, promptly provide the identity and contact details of the competent supervisory authority without undue delay.

(e) For Clause 17 (Governing law) Option 2 (for Modules Two and Three) is selected to read as follows:

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established or operates. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden, without reference to its conflicts of law principles.

(f) Clause 18 (Choice of forum and jurisdiction) is modified to read as follows:

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

(b) The Parties agree that those shall be the courts of the EU Member whose laws have been agreed upon as the governing law under Clause 17.

(c) 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.

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

(g) Clause 19 is added to read as follows:

These Clauses are to be interpreted as extending to include countries within the European Economic Area (EEA) that are not members of the European Union (EU), insofar as Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) applies to these countries due to their EEA affiliation.

(h) **Appendix** is incorporated as is and without any modifications into this Part 1.

Part 2: UK Restricted Transfer Mechanism

For Restricted Transfers initiated by controllers-exporters and processors-exporters subject to the UK Data Protection Laws, the **Part 1** shall apply, as modified in accordance with the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the Information Commissioner effective from 21 March 2022 (Addendum), as follows:

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.

Section 1: Tables

Table 1: Parties

Start date	Effective date of the Agreement.
List of Parties	Refer to ***Appendix, Annex I, lit. 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 is as set forth in **Part 1** of this Schedule 1.

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: Refer to ***Appendix, Annex I, lit. A***
Annex 1B: Description of Transfer: Refer to ***Appendix, Annex I, lit. B***
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Refer to ***Appendix, Annex II***
Annex III: List of Sub processors (Modules 2 and 3 only): n/a

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 X Exporter ☐ neither Party

Section 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 Section 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.

Part 3: CH Restricted Transfer Mechanism

For Restricted Transfers initiated by controllers-exporters and processors-exporters subject to the Swiss Federal Data Protection Act (FADP), the **Part 1** shall apply, as modified in accordance with the FDPIC's guidance "The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts" that was published on 27 August 2021 and can be access it here. Amendments to **Part 1** are as follows:

(a) Clause 13(a) is modified to read as follows:

The Office of the Federal Data Protection and Information Commissioner (FDPIC) is the supervisory authority. For inquiries or further information, the FDPIC can be reached at:

Office of the Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH - 3003 Berne

Telefon: +41 (0)58 462 43 95
Telefax: +41 (0)58 465 99 96
https://www.edoeb.admin.ch/edoeb/en/home/adresse.html

(b) Clause 17 (Governing law) is modified to read as follows:

These Clauses shall be governed by the Swiss laws.

(c) Clause 18 (Choice of forum and jurisdiction) is modified to read as follows:

(a) Any dispute arising from these Clauses shall be resolved by the competent Swiss courts with jurisdiction in the data exporter's place of business.

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the competent Swiss courts with jurisdiction in the data subject's habitual residence.

(d) Clause 19 is modified to read as follows:

All references to the GDPR in these Clauses and Appendix are to be understood as references to the FADP, as applicable.

Part 4: Other Jurisdiction's Restricted Transfer Mechanism

For Restricted Transfers initiated by controllers-exporters and processors-exporters subject to Data Protection Laws and Regulations other than GDPR, the UK Data Protection Laws, and FADP, the **Part 1** shall apply, modified as follows:

(a) Clause 13(a) is modified to read as follows:

The supervisory authority with responsibility for ensuring compliance by the data exporter with Data Protection Laws and Regulations is the competent supervisory authority.

(b) Clause 17 (Governing law) is modified to read as follows:

These Clauses shall be governed by Swiss laws, except where Data Protection Laws and Regulations preclude this. In such case, the laws of the jurisdiction where the data exporter

is established shall govern.

(c) Clause 18 (Choice of forum and jurisdiction) is modified to read as follows:

Any dispute arising from these Clauses shall be resolved in the competent courts of the jurisdiction selected as the governing law under Clause 17.

(d) Clause 19 is modified to read as follows:

All references to the GDPR in these Clauses and Appendix are to be understood as references to Data Protection Laws and Regulations, as applicable.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Module	Data exporter(s):	Data importer(s):
MODULE TWO: Transfer controller to processor	Customer using the Service. Activities relevant to the Personal Data transferred under these Clauses. Transfer of contact details in order to register to use the Services. Transfer of Personal Data as required to perform support and de-bugging activities. Role: Controller	Hexagon Aura Reality AG, Heinrich-Wild-Strasse 201, 9435 Heerbrugg, Switzerland Sandro Schefer, Privacy Officer. Email: privacy.ven@hexagon.com Activities relevant to the data transferred under these Clauses. Utilising the contact details to provide Services as per Agreement. Utilising data provided to support and de-bug the application after purchase. Role: Processor
MODULE THREE: Transfer processor to processor	Customer selling the Service to its clients. Activities relevant to the Personal Data transferred under these Clauses. Transfer of contact details in order to register to use the Services and to register clients. Transfer of Personal Data as required to perform support and de-bugging activities. Role: Processor	Hexagon Aura Reality AG, Heinrich-Wild-Strasse 201, 9435 Heerbrugg, Switzerland Sandro Schefer, Privacy Officer Email: privacy.ven@hexagon.com Activities relevant to the data transferred under these Clauses. Utilising the contact details to provide Services in as per the Agreement Utilising data provided to support and de-bug the application after purchase. Role: Sub-processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Distributors, Clinic staff including doctors and support staff, and patients of clinics. . . . . .

Categories of personal data transferred

For AURA: Contact Data such as: Contact Person Name, Email Address, Address, and Phone Number. Screen grabs of the application, Artifacts as generated by the application

In addition, for AURA Cloud Services: system access / usage / authorization data, any application-specific data transferred or entered into AURA Cloud

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

Not required by the Service, Section 9 of the DPA applies. . . . . .

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

On a continuous basis as requested by the data exporter. . . . . .

Nature of the processing

The Personal Data provided will be Processed in the provision of the application and cloud services as well as provide post-sales support and product enhancements . . . . . .

Purpose(s) of the data transfer and further processing

To fulfil contractual obligations as set out in the Agreement . . . . . .

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

Personal Data shall be retained for the duration of the commercial relationship with the clients. Whereafter, Personal Data shall be deleted. Personal Data shall also be deleted upon termination of the Service by either Party. Personal Data Processed for de-bugging will be deleted ninety (90) days after the ticket is closed.. . . . . .

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

Sub processors will Process Personal Data to the same extent as HAR. . . . . .

C. COMPETENT SUPERVISORY AUTHORITY

Refer to Clause 13 in Part 1, 2, 3 or 4, as applicable.

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

CONFIDENTIALITY (ART. 32 (1) (b) GDPR)

- Physical Access Control: No unauthorised access to data processing facilities, e.g., magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV systems.
- Electronic Access Control: No unauthorised use of the data processing and data storage systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media.
- Internal Access Control (permissions for user rights of access to and the amendment of data): No unauthorised reading, copying, changes or deletions of data within the system, e.g., rights authorisation concept, need-based rights of access, logging of system access events.
- Isolation Control: The isolated processing of data, which is collected for differing purposes, e.g., multiple Controller support, sandboxing.
- Pseudonymisation (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR): The processing of personal data in such a method/way, to ensure that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

INTEGRITY (ART. 32 (1) (b) GDPR)

- Data Transfer Control: No unauthorised reading, copying, changes or deletions of data with electronic transfer or transport, e.g. virtual private networks (VPN), electronic signature. Encryption during transfer and storage.
- Data Entry Control: Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g., logging, document management.

AVAILABILITY AND RESILIENCE (ART. 32 (1) (b) GDPR)

- Availability Control: Prevention of accidental or willful destruction or loss, e.g., backup strategy (online/offline; on-site/offsite), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning.
- Rapid Recovery (Art. 32 (1) (c) GDPR);

PROCEDURES FOR REGULAR TESTING, ASSESSMENT, AND EVALUATION (ART. 32 (1) (d) GDPR; ART. 25 (1) GDPR)

- Data Protection Management.
- Incident Response Management.
- Data Protection by Design and Default (Art. 25 (2) GDPR).
- Order or Contract Control
- No third-party data processing as per Art. 28 GDPR without corresponding instructions from the Controller, e.g., clear and unambiguous contractual arrangements, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.

For data transfers to (sub)processors, at least equivalent security measures shall be applied.

SCHEDULE 2: DESCRIPTION OF PROCESSING

ANNEX I

List of parties

Roles	Direct Business	Indirect Business
Controller	Customer using the Service.	
Processor	Hexagon Aura Reality AG Heinrich-Wild-Strasse 201 9435 Heerbrugg, Switzerland Sandro Schefer, Privacy Officer, Email: privacy.ven@hexagon.com	Customer selling the Service to its clients.
Sub-processor	n/a	Hexagon Aura Reality AG Heinrich-Wild-Strasse 201 9435 Heerbrugg, Switzerland Sandro Schefer, Privacy Officer Email: privacy.ven@hexagon.com

ANNEX II

Description of the processing

Categories of data subjects whose personal data is transferred

Distributors, Clinic staff including doctors and support staff, and patients of clinics. . . . . .

Categories of personal data transferred

For AURA: Contact Data such as: Contact Person Name, Email Address, Address, and Phone Number. Screen grabs of the application, Artifacts as generated by the application

In addition, for AURA Cloud Services: system access / usage / authorization data, any application-specific data transferred or entered into AURA Cloud

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

Not required by the Service, Section 9 of the DPA applies. . . . . .

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

On a continuous basis as requested by the data exporter. . . . . .

Nature of the processing

The Personal Data provided will be Processed in the provision of the application and cloud services as well as provide post-sales support and product enhancements . . . . . .

Purpose(s) of the data transfer and further processing

To fulfil contractual obligations as set out in the Agreement . . . . . .

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

Personal Data shall be retained for the duration of the commercial relationship with the clients. Whereafter, Personal Data shall be deleted. Personal Data shall also be deleted upon termination of the Service by either Party. Personal Data Processed for de-bugging will be deleted ninety (90) days after the ticket is closed.. . . . . .

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

Sub processors will Process Personal Data to the same extent as HAR. . . . . .

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

CONFIDENTIALITY (ART. 32 (1) (b) GDPR)

- Physical Access Control: No unauthorised access to data processing facilities, e.g., magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV systems.
- Electronic Access Control: No unauthorised use of the data processing and data storage systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media.
- Internal Access Control (permissions for user rights of access to and the amendment of data): No unauthorised reading, copying, changes or deletions of data within the system, e.g., rights authorisation concept, need-based rights of access, logging of system access events.
- Isolation Control: The isolated processing of data, which is collected for differing purposes, e.g., multiple Controller support, sandboxing.
- Pseudonymisation (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR): The processing of personal data in such a method/way, to ensure that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

INTEGRITY (ART. 32 (1) (b) GDPR)

- Data Transfer Control: No unauthorised reading, copying, changes or deletions of data with electronic transfer or transport, e.g. virtual private networks (VPN), electronic signature. Encryption during transfer and storage.
- Data Entry Control: Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g., logging, document management.

AVAILABILITY AND RESILIENCE (ART. 32 (1) (b) GDPR)

- Availability Control: Prevention of accidental or willful destruction or loss, e.g., backup strategy (online/offline; on-site/offsite), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning.
- Rapid Recovery (Art. 32 (1) (c) GDPR);

PROCEDURES FOR REGULAR TESTING, ASSESSMENT, AND EVALUATION (ART. 32 (1) (d) GDPR; ART. 25 (1) GDPR)

- Data Protection Management.
- Incident Response Management.
- Data Protection by Design and Default (Art. 25 (2) GDPR).
- Order or Contract Control
- No third-party data processing as per Art. 28 GDPR without corresponding instructions from the Controller, e.g., clear and unambiguous contractual arrangements, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.

For data transfers to (sub)processors, at least equivalent security measures shall be applied.

ANNEX IV

Agreed list of Sub-processors in accordance with Section 5.2. of the DPA

Entity Name/Country of establishment	Sub-processing Activity	Processing Location(s)
Hexagon Capability Center Pvt Ltd /India	Trouble shooting, support, de-bugging and further development of the Service	India
Hexagon Geosystems India Pvt Ltd/India	Trouble shooting, support, de-bugging and further development of the Service	India
Leica Geosystems AG/Switzerland .	Trouble shooting, support, de-bugging and further development of the Service	Switzerland
Hexagon Technology Center GmbH/Switzerland	Trouble shooting, support, de-bugging and further development of the Service	Switzerland
Technodigit SARL/France	Trouble shooting, support, de-bugging and further development of the Service	France
Melown Technologies SE/Switzerland	Trouble shooting, support, de-bugging and further development of the Service	Switzerland
Tacticaware s.r.o/Czech Republic	Trouble shooting, support, de-bugging and further development of the Service	Czech Republic

Intergraph Polska Sp. z o.o. ul./Poland	Trouble shooting, support, de-bugging and further development of the Service	Poland
deepsense.ai Sp. z o.o./Poland	Trouble shooting, support, de-bugging and further development of Aura 3D Imaging System	Poland
Microsoft Ireland Operations Limited /Ireland	Host back-end web services, database, azure blob , portal web services and B2C SaaS offering for authentication, provision of AURA Cloud	Europe