Data Processing Addendum

This Data Processing Addendum (the "DPA") forms part of the Master Services Agreement (the "Agreement") between Evolv Technologies Holdings, Inc., D/B/A Evolv Technology, Inc., ("Evolv") and Customer ("Customer").

This DPA is incorporated into the Agreement between Evolv and Customer and applies to Evolv's Processing of Personal Data in connection with Evolv's provision of the Products and related Software Services and Customer Services (as defined in the Agreement) to Customer. In the event of any inconsistency between the DPA and the Agreement as to Evolv's Processing of Personal Data, the DPA shall control.

For purposes of this DPA, the following terms and those defined within the body of this DPA apply.

1. DEFINITONS

1.1 In this DPA, the terms "**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in applicable Data Protection Laws with the same or equivalent terms, and the following words and expressions shall have the following meanings unless the context otherwise requires:

1.2 "**Customer Personal Data**" means the Personal Data described in **Annex 1** of **Schedule 1**, and any other Personal Data that Evolv Processes on behalf of Customer in connection with Evolv's provision of the Services.

1.3 "**Data Protection Laws**" means all applicable laws, rules and regulations relating to the Processing of Personal Data as amended, repealed, consolidated or replaced from time to time.

1.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Data by Evolv that compromises the security, confidentiality or integrity of such Customer Personal Data.

1.5 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.6 "**Subprocessor**" means any Processor engaged by Evolv to Process Customer Personal Data on Evolv's behalf.

1.7 "**Third Country**" means any country outside of a country in which the Data Protection Laws restrict transfers of Personal Data to destinations outside of that country, except where the Data Protection Laws and applicable regulatory authorities of the originating country adopted an adequacy decision regarding the Data Protection Laws of the destination country such that transfers of Personal Data to that destination country are not restricted.

1.8 "**UK Addendum**" means United Kingdom ("UK") Information Commissioner's ("ICO") International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0 in force 21 March 2022.

Capitalized terms used in this DPA and not defined above shall have the meaning set forth in the Agreement.

2. DATA PROCESSING

2.1 Evolv will only Process Customer Personal Data in accordance with the Agreement and any Order Document, to the extent necessary to provide the Customer Services and Software Services (collectively, "Services") to Customer, and Customer's written instructions, including with respect to transfers of Customer Personal Data, unless Processing is required by applicable Data Protection Laws, in which case Evolv shall, to the extent permitted by applicable law, inform Customer of that legal requirement before so Processing that Customer Personal Data. Evolv shall not Process Customer Personal Data outside of the direct business relationship between Customer and Evolv. Evolv shall not 'sell' or 'share' (as such terms may be specifically defined in applicable Data Protection Laws) Customer Personal Data. To the extent required by applicable Data Protection Laws, Evolv certifies that it understands the foregoing restrictions and will comply with them. The Agreement, DPA, and any Order Document (subject to any changes to the Services) shall be Customer's complete and final instructions to Evolv in relation to the Processing of Customer Personal Data. Processing outside the scope of the foregoing will require prior written agreement between Customer and Evolv on additional instructions for Processing and may be subject to additional fees. As part of the Services, and in compliance with Data Protection Law, Evolv may Process certain Customer Personal Data of select customers to optimize and improve the Service.

2.2 Customer shall provide all applicable notices to Data Subjects required under applicable Data Protection Laws for the lawful Processing of Customer Personal Data by Evolv in accordance with the Agreement, including notices for capturing images of Data Subjects. Customer shall obtain and maintain throughout the term of the Agreement any required consents and/or authorizations related to its provision of, and Evolv's processing of, Customer Personal Data as part of the Services, including for capturing images of Data Subjects. If Customer is not required by Data Protection Laws to obtain and maintain valid consent from Data Subjects, Customer will otherwise obtain and maintain a valid legal basis in accordance with Data Protection Laws to Process Customer Personal Data and for providing such data to Evolv for Processing under the Agreement.

2.3 For the avoidance of doubt, Customer's instructions for the processing of Customer Personal Data shall comply with the Data Protection Laws. Customer acknowledges that Evolv is reliant on Customer for direction as to the extent to which Evolv is entitled to use and Process Customer Personal Data. Consequently, Evolv will not be liable for any claim brought against Customer by a Data Subject arising from any act or omission by Evolv to the extent that such act or omission resulted from Customer's instructions or Customer's use of the Services.

2.4 Unless set forth in an Order Document, Customer Data may not include any sensitive or special data that imposes specific data security or data protection obligations on Evolv in addition to or different from those specified in the Documentation or which are not provided as part of the Services.

2.5 If applicable Data Protection Laws recognize the roles of Controller and Processor as applied to Customer Personal Data then, as between Customer and Evolv, Customer acts as Controller and Evolv acts as a Processor (or subprocessor, as the case may be) of Customer Personal Data.

2.6 As required by applicable Data Protection Laws, if Evolv believes any Customer instructions to Process Customer Personal Data will violate applicable Data Protection Laws, or if applicable Data Protection Laws require Evolv to process Customer Personal Data relating to data subjects in a way that does not comply with Customer's documented instructions, Evolv shall notify Customer in writing, unless applicable Data Protection Laws prohibit such notification, provided Evolv is not responsible for performing legal research or providing legal advice to Customer.

2.7 Evolv shall Process Customer Personal Data for the duration of the provision of Services in accordance with the Agreement and thereafter only as set forth in the Agreement and this DPA.

2.8 Each Party will comply with Data Protection Laws applicable to such Party in connection with the Agreement and this DPA.

3. SUBPROCESSORS

3.1 Consent to Subprocessor Engagement. Customer generally authorizes the engagement of third parties as Subprocessors. For the avoidance of doubt, this authorization constitutes Customer's prior written consent to the subprocessing of Customer Personal Data for purposes of Clause 9, Option 2 of the Standard Contractual Clauses and any similar requirements of other data transfer mechanisms.

3.2 Information about Subprocessors. A current list of Subprocessors is available at https://learn.evolvtechnology.com/express-subprocesser-list ("Subprocessor List"), and may be updated by Evolv from time to time in accordance with this DPA. Customer may sign up to receive notices of additions to the Subprocessor List by completing the email sign-up process on the Subprocessor List web page referenced above.

3.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Evolv will:

(a) execute with Subprocessors a written agreement providing:

(i) the Subprocessor only Processes Customer Personal Data to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement and this DPA; and

(ii) the Subprocessor utilize the same level of data protection and security with regard to its Processing of Customer Personal Data as are described in this DPA.

(b) be responsible for the Subprocessor's violations of this DPA or Data Protection Laws in relation to the services such Subprocessor provides to Evolv to the extent Evolv would be liable for the same violations under the terms of the Agreement.

3.4 Opportunity to Object to Subprocessor Changes**.** Customer may, on reasonable and objective grounds, object to Evolv's use of a new Subprocessor by providing Evolv with written notice within fifteen (15) days after Evolv has provided notice to Customer as described herein with documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA or Data Protection Laws ("Objection"). In the event of an Objection, Customer and Evolv will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Data Protection Laws. To the extent Customer and Evolv do not reach a mutually acceptable resolution within a reasonable timeframe, Evolv will use reasonable endeavors to make available to Customer a change in the Services or will recommend a commercially reasonable change to the Services to prevent the applicable Subprocessor from Processing Customer Personal Data. If Evolv is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, Evolv and Customer shall escalate to their applicable executive or senior leadership to discuss the matter in good faith and determine an appropriate resolution and next steps.

4. INTERNATIONAL TRANSFERS

4.1 In accordance with Customer's instructions under Section 2, Evolv may Process Customer Personal Data on a global basis as necessary to provide the Services, including for IT security purposes, maintenance and provision of the Services and related infrastructure, technical support, and change management.

4.2 To the extent that the Processing of Customer Personal Data by Evolv involves the transfer of such Customer Personal Data from a country whose Data Protection Laws restrict the transfer of Personal Data to Third Countries, then such transfers shall be subject to the protections and provisions of the Standard Contractual Clauses (for which the SCC Appendix is attached to this DPA in Schedule 1), the UK Addendum for transfers from the UK to Third Countries, or other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Data Protection Laws.

4.3 Customer shall be deemed to have signed the SCC in Schedule 1, Annex I in its capacity of "data exporter" and Evolv in its capacity as "data importer." Module Two of the SCC shall apply to the transfer. For purposes of Clauses 17 and 18 of the SCCs, the Parties select the Netherlands. To the extent such a transfer includes Personal Data subject to Data Protection Laws of Switzerland, the Standard Contractual Clauses shall be adapted to use for Switzerland (where the Swiss Federal Act on Data Protection shall apply as the applicable Data Protection Law, Clauses 17 and 18 of the SCCs shall refer to Switzerland, and Data Subjects in Switzerland shall be able to avail themselves of any rights conferred by the Standard Contractual Clauses).

4.4 The SCC, or UK Addendum, as applicable, will cease to apply if Evolv has implemented an alternative recognized compliance mechanism for the lawful transfer of personal data in accordance with applicable Data Protection Laws.

4.5 In the event of any conflict between any terms in the SCC or UK Addendum, as applicable, and the DPA, the SCC or UK Addendum, as applicable, shall prevail to the extent of the conflict.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 Evolv Security Obligations**.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Evolv shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk of the Processing, including the measures set out in Schedule 1. Evolv may update its security practices from time to time but will not materially decrease the overall security of the Services during the term of the Agreement. Such measures shall include process for regularly testing, assessing, and evaluating the effectiveness of the measures.

5.2 Security Audits.

(a) Evolv will, upon Customer's written request, verify its compliance with its obligations in this DPA by first providing to Customer for its review documentation regarding the same and, if such documentation is not reasonably sufficient to address Customer's inquiries, participate in and contribute to audits as set forth below.

(b) Customer may, upon at least 30 days' advance written notice and at reasonable times, audit (either by itself or using independent third-party auditors) Evolv's compliance with the security measures set out in this DPA solely for the purpose of confirming Evolv's compliance with its obligations under this

DPA. Evolv shall reasonably assist with any audits conducted in accordance with this Section 5.2. Such audits may be carried out once per year, or more often if required by Data Protection Law or Customer's applicable Supervisory Authority.

(c) Any third party engaged by Customer to conduct an audit must be pre-approved by Evolv (such approval not to be unreasonably withheld) and sign Evolv's confidentiality agreement. Customer must provide Evolv with a proposed audit plan at least two weeks in advance of the audit, after which Customer and Evolv shall discuss in good faith and finalize the audit plan prior to commencement of audit activities.

(d) Audits may be conducted only during regular business hours, in accordance with the finalized audit plan and Evolv's security and other policies, and may not unreasonably interfere with Evolv's regular business activities. Evolv is not required to grant access to its premises or systems for the purposes of such an audit to any individual unless they produce reasonable evidence of identity and authority. Customer shall reimburse Evolv for any costs or expenses incurred by Evolv in granting access to its data processing facilities.

(e) Information obtained or results produced in connection with an audit are Evolv confidential information and may only be used by Customer to confirm compliance with this DPA and for complying with its requirements under Data Protection Laws.

(f) Customer may request that Evolv audit a Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Customer in obtaining a third-party audit report concerning the Subprocessor's operations) to verify compliance with the Subprocessor's obligations.

(g) Without prejudice to the rights granted in Section (b) above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report or attestation letter issued by a qualified third party auditor within the prior twelve months and Evolv provides such report or attestation letter to Customer confirming there are no known material changes in the controls audited, Customer agree to accept the findings presented in the third party audit report or attestation letter in lieu of requesting an audit of the same controls covered by the report.

5.3 Upon Customer's written request, Evolv shall make available all information reasonably necessary to demonstrate compliance with this DPA as required by Data Protection Laws.

5.4 Personal Data Breach Notification.

(a) If Evolv becomes aware of and determines a Personal Data Breach has occurred, Evolv will:

(i) notify Customer of the Personal Data Breach without undue delay and, in any case, as soon as practicable after such determination, at the contact information on file, where such notification shall describe (1) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (2) the reasonably anticipated consequence of the Personal Data Breach; (3) measures taken to mitigate any possible adverse effects; and (4) other information concerning the Personal Data Breach reasonably known or available to Evolv that Customer is required to disclose to a Supervisory Authority or Data Subjects under Data Protection Laws; and

(ii) investigate the Personal Data Breach and provide such reasonable assistance to the Client (and any law enforcement or regulatory official) as required to investigate the Personal Data Breach.

5.5 Except as required by applicable Data Protection Laws, the obligations set out in Section 5.4 shall not apply to Personal Data Breaches caused by Customer.

5.6 Evolv's contact point for additional details regarding a Personal Data Breach is privacy@evolvtechnology.com. Evolv's provision of any notification of a Personal Data Breach shall not constitute an admission of fault.

5.7 Customer is solely responsible for fulfilling any Personal Data Breach notification obligations applicable to Customer. Customer and Evolv shall work together in good faith within the timeframes for Customer to provide Personal Data Breach notifications in accordance with Data Protection Laws to finalize the content of any notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Laws. Evolv's prior written approval shall be required for any statements regarding, or references to, Evolv made by Customer in any such notifications.

5.8 Evolv Employees and Personnel**.** Evolv shall treat Customer Personal Data as the Confidential Information of Customer, and shall put procedures in place to ensure that:

(a) access to Customer Personal Data is limited to those employees or other personnel who have a business need to have access to such Customer Personal Data; and

(b) any employees or other personnel with access to Customer Personal Data have committed themselves to confidentiality of Customer Personal Data or are under an appropriate statutory obligation of confidentiality and do not Process such Customer Personal Data other than in accordance with this DPA.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 Save as required (or where prohibited) under applicable law, Evolv shall promptly notify Customer of any request received by Evolv or any Subprocessor from a Data Subject in respect of their Personal Data included in Customer Personal Data ("Data Subject Request") and shall not respond to the Data Subject Request where the Data Subject identifies Customer as its Controller. If a Data Subject does not identify a Controller, Evolv will instruct the Data Subject to identify and contact the relevant Controller.

6.2 Where applicable, and taking into account the nature of the Processing, Evolv shall use reasonable endeavors to assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to Data Subject Requests as required by Data Protection Laws. In order to receive such assistance, Customer shall submit a support request to correct, delete, block, access or copy the Personal Data of a Data Subject.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, Evolv shall provide reasonable assistance to Customer with any data protection impact assessments and with any prior consultations to any Supervisory Authority of Customer, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to Evolv.

7.2 Such cooperation and assistance are provided to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Evolv. Evolv may fulfil its above obligations by providing Customer with documentation regarding its Processing operations.

8. RETENTION AND DELETION OF PERSONAL DATA

8.1 During the Term, the Services retain Personal Data for a period of time based on Customer's configuration of the Services. The configuration settings may prescribe, for example, that certain Personal Data are only retained in the Equipment system memory and erased on reboot, or that that certain Personal Data are retained for so long as the applicable Services component has sufficient disk space, or that certain Personal Data are stored in the Services for seven days. Depending on Customer's configuration of the Services and Equipment, Customer shall have access to Personal Data for a period of time after termination or expiration of the Agreement.

8.2 Subject to Section 8.3 below, where deletion of Personal Data is not possible, Evolv will sufficiently de-identify Customer Personal Data that is reasonably capable of deidentification such that it is no longer Personal Data, except for compliance, audit, security, or Equipment configuration or Service optimization purposes.

8.3 Evolv and its Subprocessors may retain Customer Personal Data to the extent required by applicable laws.

9. GENERAL

9.1 With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including but not limited to the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations for Customer Personal Data of a Data Subject. Notwithstanding the foregoing, and solely to the extent applicable to any protected health information (as defined under and regulated by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA")) ("HIPAA Data"), if there is any inconsistency or conflict between this DPA and a Business Associate Agreement between Evolv and Customer (the "BAA"), then the BAA shall prevail to extent the inconsistency or conflict relates to such HIPAA Data.

9.2 Evolv may share and disclose Customer Personal Data and other data of Customer in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Evolv's business by or to another company, including the transfer of contact information and data of customers, partners and end users.

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

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter

Name:	The data exporter is the entity identified as "Customer" in the DPA
Address:	As set forth in the Agreement
Contact person:	As set forth in the Notices provision in the Agreement or Order Document
Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA or Agreement, as applicable
Role:	Controller, except when processing data on behalf of another entity, in which case data exporter is a Processor

Data importer

Name:	The data importer is the entity identified as "Evolv" in the DPA
Address:	As set forth in the Agreement
Contact person:	privacy@evolvtechnology.com
Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA or Agreement, as applicable
Role:	Processor, or Subprocessor if data exporter is a Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Data exporter's contacts including its employees, contractors, suppliers and subcontractors and other personnel, and its customers, patrons, and other visitors. Data exporter will prevent the sharing or transfer to data importer of Personal Data of patients unless data importer has agreed in writing.
Categories of personal data transferred:	Depending on data exporter's configuration of the data importer's Services categories of personal data may include contact information, images, location information, and application/website usage information.
Sensitive categories of data (if appropriate):	N/A
The frequency of the transfer:	As set forth in the Agreement
Nature of the processing:	The subject-matter and nature of the processing of data exporter Personal Data by data importer is for the provision of the Services to the data exporter under the Agreement.
Purposes of the data transfer and further processing:	Refer to DPA.
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 will be processed for the duration of the Agreement, subject to Section 10 of the DPA
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Refer to DPA and the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority shall be the Netherlands, or the UK ICO for matters related to data subjects in the UK.

ANNEX II

Evolv agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by applicable data protection law(s). Such measures will include:

1. Establish and maintain an information security program designed to (i) protect the security and confidentiality of data exporter's Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of data exporter's Personal Data; (iii) protect against unauthorized access to or use of data exporter's Personal Data; and (iv) ensure the proper disposal of data exporter's Personal Data.

2. Provide security awareness and training programs delivered not less than annually, for all Evolv personnel who access data exporter's Personal Data.

3. Maintain controls that provide reasonable assurance that access to data importer's physical servers at its production data center ("Systems") is limited to properly authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. Logging and monitoring of unauthorized access attempts made to the Systems by the data center security personnel, and camera surveillance systems at critical internal and external entry points to the data center.

4. Maintain policies and procedures designed to protect the confidentiality, integrity, and availability of Personal Data and protect it from unauthorized disclosure, alteration, or destruction. For clarity, data importer does not control data exporter's user-facing configuration of any data importer software and is not responsible for any of the foregoing obligations and protections to the extent they are controlled by data exporter's configuration of the software. Data importer will provide guidance on the recommended configuration of user-facing software.

5. Maintain a security incident response plan that includes procedures to be followed in the event of any incident that results in a Personal Data Breach. The procedures include:

    a. Roles and responsibilities: formation of an internal incident response team with a response leader

    b. Investigation: assessing the risk the Personal Data Breach poses and determining which customers may be affected

    c. Communication: internal reporting as well as a notification process to data importer customers and other applicable third parties.

6. Implement storage and transmission security measures designed to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network. Such measures include requiring NIST acceptable encryption of any Personal Data stored on desktops, laptops or other mobile computer devices. Data importer will encrypt sensitive data when transmitted over public networks.

ANNEX III

The data exporter has authorized the use of the following subprocessors:

Please see https://learn.evolvtechnology.com/express-subprocesser-list

Version: December 1, 2022