Saudi Data Processing Addendum

This Saudi Data Processing Addendum (the "**DPA**") forms part of the Service Terms for Evolv Products (the "**Service Terms**"), to the extent applicable, between you ("**Customer**") and Evolv Technologies, Inc. ("**Evolv**").

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 Professional Services (to the extent applicable) 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 " **Competent 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all applicable laws, rules and regulations relating to the Processing of Personal Data including the PDPL as amended, repealed, consolidated or replaced from time to time.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**" are the Saudi Contractual Clauses issued by SDAIA.

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 "**PDPL**" means the Saudi Personal Data Protection Law, issued by Royal Decree No. M/19 dated 09/02/1443 AH and amended by Royal Decree No. M/148 dated 05/09/1444 AH, together with its Implementing Regulations.

1.9 "**SDAIA**" means the Saudi Data and Artificial Intelligence Authority.

1.10 "**KSA**" means kingdom of Saudi Arabia.

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 Professional Services and/or Software (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 all applicable Data Protection Laws in the operating jursidictions. 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 and or remediation efforts of the subprocessor 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), DPA for transfers from KSA 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." Template Two of the SCC issued by SDAIA shall apply to the transfer.

4.4 The SCC, or DPA , 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 DPA, as applicable, and the DPA, the SCC, 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 per a timeline mutually agreeable to Evolv and the Customer, 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 DP, provided that such an audit will not place an inordinate resource burden on Evolv 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. The timeline and schedule commits for such an audit must be negotiated at each instance of such a request.

(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. The subprocessor may, in lieu of the audit, submit existing compliance audit reports and certifications whose security standards (e.g., ISO27001, SOC2 etc.) conform to the objectives of the DPA. Customer shall have the discretion to accept or reject such reports and insist on a new audit of the subprocessor.

(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.

(h) In the absence of a recent audit report based on SOC, ISO, NIST, PCI DSS standards, Evolv might, in good faith, request a compliance plan deadline to initiate/conduct a fresh audit to the effect of this request. In such event, Evolv must commission an audit submit a report thereof no later than 12 months from the data of request.

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 and the extent that the effort required by Evolv to fulfil such requests could be negotiated with mutual cooperation. 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 upto seven, fourteen or thirty days depending on the specific storage artefact in the Express solution and its components. If, during the course of product evolution, Evolv changes these retention policies which could be deemed as a weaker security posture by the Customer, Evolv will make available all the foregoing options for retaining security posture which is compatible with the terms in the DPA. 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 and the PDPL

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

Protection of Transferred Personal Data

Standard Contractual Clauses

Clause (1) Purpose and Scope

1. The purpose of these Clauses is to ensure that an appropriate level of Personal Data protection equivalent to the level of protection applicable under the Personal Data Protection Law and its Implementing Regulations is applied in the absence of an appropriate level of Personal Data protection outside the Kingdom by specifying the obligations of the parties involved in the transfer of Personal Data to a country or international organization that does not have an appropriate level of Personal Data protection. Appendix (1) shows the data for both Data Exporters and Data Importers.
2. These Clauses apply to the transfer of Personal Data as specified in Appendix (2) ("Personal Data to be Transferred or Disclosed").

Clause (2) Modification and Impact

1. These Clauses set out appropriate safeguards, including rights of complaint by Personal Data Subjects, and cannot be amended except to select the appropriate template or to add or update information in the appendix.
2. The parties may incorporate these Clauses into a comprehensive agreement or add other clauses or additional guarantees, provided they do not directly or indirectly conflict with these Clauses or infringe on the fundamental rights of Personal Data Subjects.
3. These Clauses do not relieve any party from its obligations under the Law and Regulations, nor do they prejudice the provisions of the Laws and Regulations in force in the Kingdom or agreements to which the Kingdom is a party.

Clause (3) Rights of Personal Data Subjects

1. These Standard Contractual Clauses are without prejudice to the rights of Personal Data Subjects under the Law and Regulations.
2. Personal Data Subjects whose Personal Data is transferred from the parties based on these Standard Contractual Clauses may notify the Competent Authority ("Saudi Data & AI Authority") if they become aware of any violation of these Standard Contractual Clauses.

Clause (4) Interpretation

1. Unless the context requires otherwise, the words and phrases used in these Clauses shall have the meanings assigned to them in Article (1) of the Personal Data Protection Law issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH, Article (1) of the Implementing Regulation of the PDPL and Article (1) of the Regulation on the Transfer of Personal Data Outside the Kingdom.
2. These Clauses must be read and interpreted in light of and in accordance with the provisions of the Law and Regulations referred to in paragraph (a) of this Article, and may not be interpreted in any other way that is inconsistent with the provisions of the Law and Regulations.

Clause (5) Conflict

1. In the event of a conflict between these Clauses and any provision in any other agreement between the parties, these Clauses shall prevail.

Clause (6) Details of Transfers

1. The transfer(s), as well as the categories of Personal Data and the purposes of the transfers, are described in the Appendix.

Clause (7) Addition of New Parties

1. Any Personal Data Importer or Personal Data Exporter who is not a party to these Standard Clauses may join these Standard Contractual Clauses by completing and signing Appendix (1), with the consent of the existing parties. The Joining Entity shall be either the Personal Data Importer or the Personal Data Exporter.
2. Once Appendix (1) has been completed and signed, the Joining Entity shall be a party to these Clauses, and the newly Joined Entity shall, as of the date of joining, and assume the responsibilities depending on the nature of the Personal Data processing and transfer operations that occurred on or after the date of joining, and shall be entitled to exercise the rights and obligations corresponding to its role as defined in these Clauses.

Clause (8) Governing Law and Jurisdiction

1. These Standard Contractual Clauses shall be governed by the applicable laws of the Kingdom of Saudi Arabia. Any dispute arising from the application of the provisions of these Clauses shall fall under the jurisdiction of the Kingdom and

be vested in its courts. The Personal Data Importer, under these Standard Contractual Clauses, agrees to submit to the jurisdiction of the Kingdom of Saudi Arabia.

Clause (9) Compliance with the Requests of the Competent Authority

1. Each party agrees to comply with any requests from the Competent Authority in relation to these Standard Contractual Clauses or the processing of transferred Personal Data.
2. The Personal Data Importer agrees and commits to cooperate with the Competent Authority and comply with all its requests and inquiries and provide the necessary documents and information to ensure compliance with the Standard Contractual Clauses.
3. The Personal Data Importer agrees to abide by the measures adopted by the Competent Authority, including corrective measures and compensation.

Clause (10) Compensation

1. If any dispute arises between the Personal Data Subject and a party regarding compliance with the Standard Contractual Clauses, that party shall use all necessary means to settle the dispute amicably with the Personal Data Subject, and all parties shall inform each other of the existence of such dispute to ensure that it is resolved in cooperation with each other.
2. The Personal Data Subject may submit to the Competent Authority any complaint arising from the application of the provisions of these Standard Contractual Clauses, in accordance with the procedures for submitting complaints specified by the Law and Regulations.
3. The Personal Data Subject has the right to claim before the competent court for compensation for material or moral damage in proportion to the magnitude of the damage arising from the application of these Standard Contractual Clauses.

Clause (11) Personal Data Security

1. All parties shall take the necessary organizational, administrative, and technical measures that ensure to maintain the privacy of personal Data against any breach at all stages of processing, including personal data security during the transfer process. In assessing the appropriate level of security, the Parties shall take into account the current state of technology, implementation costs, and the nature of the Personal Data transferred, as well as the nature, scope, context, purposes, the risks involved in the processing of the Personal Data, and specifically consider the application of encryption or de-identification, including during Personal Data transfer, where the purpose of the data processing can be achieved in this way.
2. The Personal Data Exporter shall assist the Personal Data Importer in fulfilling the necessary data security requirements, and in the event of any Personal Data breach in relation to the transferred Personal Data processed by The Personal Data Exporter under these Standard Contractual Clauses, The Personal Data Exporter shall notify the Personal Data Importer without delay after becoming aware of such breach and shall assist the Personal Data Importer in containing such breach.
3. The Data Exporter ensures that persons authorized to process the transferred Personal Data are bound by confidentiality and non-disclosure under an appropriate legal obligation of confidentiality and non-disclosure.

Clause (12) Duration and Termination

1. If, for any reason, the personal Data Importer is unable to fulfill its obligations under these Standard Contractual Clauses, it must inform The Personal Data Exporter within forty-eight (48) hours from the time it becomes aware of this.

2. In the event that the personal Data Importer violates these Standard Contractual Clauses or is unable to comply with them, the personal Data Exporter shall immediately cease the transfer of Personal Data to the Personal Data Importer until the Personal Data Importer ensures its return to compliance again, provided that the Personal Data Importer shall be given a period of (30) days, extendable for a similar maximum period, to prove its ability to comply with these Clauses, and if the period expires without achieving this, the two parties shall agree to terminate the contract, without any liability for the Personal Data Exporter or Controller, as the case may be.
3. The Personal Data Exporter or Controller, as the case may be, shall ensure that all Personal Data previously transferred to the Personal Data Importer is fully destroyed before terminating the Standard Contractual Clauses under paragraph (b) above. It shall also ensure that any copies it has of such personal data are destroyed.
4. The Personal Data Importer must document the destruction of the data, and this documentation must be provided to the Personal Data Exporter or controller upon request.
5. The Personal Data Importer must continue to ensure - until the data is destroyed - that it complies with these Standard Contractual Clauses.

Clause (13) Protection of Transferred Personal Data

1. The Personal Data Exporter and the Personal Data Importer shall process the transferred Personal Data according to the nature and purposes of the transfer as follows:

Template: Controller to Processor

1. Processing Instructions

The Personal Data Importer shall only process the transferred Personal Data based on written instructions from the Personal Data Exporter. Accordingly, if the Personal Data Importer is unable to follow the instructions, it shall inform the Personal Data Exporter in writing without undue delay.

2. Processing Restrictions

The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Appendix (2), unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

3. Compliance with the Requests of the Competent Authority

3.1 In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information in relation to transfers of Personal Data.

3.2 Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the Transferred Personal Data.

3.3 Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

4. Accuracy and Quality of Personal Data

If The Personal Data Importer realizes that any Personal Data transferred is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, in which case the Personal Data Importer shall destroy the Personal Data and notify the Personal Data Exporter accordingly, unless the Personal Data Exporter is instructed not to destroy the data because it wishes to correct the transferred Personal Data.

5. Duration of Personal Data Processing and Destruction or Recovery

5.1 The processing shall be carried out by the Personal Data Importer only for the period specified in Appendix (2). After completion of the purpose of the processing, The Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly unless otherwise instructed by the Personal Data Exporter in the following cases:

a. Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;

b. If the applicable regulations in the Kingdom or those in the operating jurisdiction of the Data Importer require the retention of the transferred Personal Data for an additional period of time.

5.2 The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

6. Personal Data Security and Personal Data Breach Notifications

6.1 The Parties shall ensure that the organizational, administrative, and technical measures specified in Appendix (3) provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulation. to the extent available at the time of such notification, in addition to the contact details for follow-up by the Personal Data Exporter. If the Personal Data Exporter realizes that the incident may cause damage to Personal Data or Personal Data Subjects or contradict their rights or interests, it shall notify the Competent Authority within (48) hours and in accordance with the requirements set out in Article (24) of the Law's Implementing Regulation.

6.2 As soon as the Personal Data Exporter receives the Data Importer's notification of a Personal Data breach incident and the incident would harm the Personal Data or the Personal Data Subject or contradict his/her rights or interests, the Personal Data Exporter must provide immediate notification in simple and clear language in accordance with the provisions of Article (24) of the Implementing Regulation to the Personal Data Subjects affected by the data breach incident, provided that the notification includes the potential risks and their nature, the measures taken or planned to be taken to contain the incident, and the contact information of the Personal Data Exporter, Data Importer, and the respective Personal Data Protection Officer of both entities, along with recommendations or consultations to aid the Data Subject in preventing or minimizing the impact of the outlined risks.

7. Sensitive Data

Without prejudice to any restrictions related to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional means of protection commensurate with the nature of the sensitive data and guarantees its protection from any risks when processing it, while ensuring that the restrictions and additional guarantees described in Appendix (2) are applied.

8. Subsequent Transfer

8.1 The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.

8.2 Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

9. Compliance with these Clauses

9.1 The Personal Data Importer shall respond to all inquiries of the Personal Data Exporter within the specified period and provide all information requested by the Personal Data Exporter, in addition to providing the Personal Data Exporter with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Personal Data Exporter to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations.

9.2 Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled.

9.3 The Personal Data Importer allows the Personal Data Exporter or its appointed representatives to audit the Data Importer's processing of Personal Data concerning the affected data subjects without undue delay upon Personal Data Exporter's request.

9.4 The Personal Data Exporter must provide the information revealed by the audit when requested by the Competent Authority.

9.5 The right of audit does not grant the Personal Data Exporter or its representatives access to any confidential information of the Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

10. Rights of Personal Data Subjects

10.1 The Personal Data Importer shall notify the Personal Data Exporter within (48) hours from the time of receipt of the request of any request received from the Personal Data Subject, and the Personal Data Importer shall not have the right to respond to such requests unless the Personal Data Exporter authorizes it to do so.

10. 2 The Personal Data Importer shall take all necessary measures in cooperation with the Personal Data Exporter to respond to the requests of Personal Data Subjects and enable them to exercise their rights under the provisions of the Law and Regulations.

10.3 The Personal Data Importer is obligated to follow all instructions issued by the Personal Data Exporter regarding the processing of the transferred Personal Data.

10.4 All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

A. **COMPETENT SUPERVISORY AUTHORITY**

If you have any concerns, or if we do not comply with the Personal Data Protection Law, you can file a complaint to Evolv Privacy at privacy@evolvtechnology.com.

If you are not satisfied with how we process your complaint, or if we fail to respond within 30 days, you can file a complaint to the Competent Authority, the Saudi Data and Artificial Intelligence Authority at:

•Website: sdaia.gov.sa.

•National Data Governance Platform (DGP) (dgp.sdaia.gov.sa).

You can exercise any of these rights by contacting us using the Contact Us page or at privacy@evolvtechnology.com.

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