DATA PROTECTION AGREEMENT
with
STANDARD CONTRACT CLAUSES

Remesh Version Date: July st, 2024

This Data Protection Agreement with Standard Contract Clauses ("**DPA**") is entered into between Remesh Inc. ("**Remesh**") (on behalf of itself and its Affiliates) and the Customer (on behalf of itself and its Affiliates) (as further defined below). The parties agree to comply with the obligations set forth in this DPA for the duration of the Agreement and for as long as Remesh Processes Customer Personal Data.

Whereas, Remesh and Customer have entered into one or more agreements relating to the provision of certain SaaS and/or other Solutions by Remesh to Customer (the "**Agreement(s)**"); and

Whereas, the parties wish to enter into this DPA to govern the Processing by Remesh of Customer Personal Data in connection with the Agreements and to govern any permitted transfers of Customer Personal Data pursuant to the SCCs which are made a part hereof.

Interpretation: This Agreement shall apply between the parties under the following scenarios *solely to the extent applicable to the relationship between the parties*:

To Customer where and to the extent the following applies:
Customer acting as the 'controller' of Customer Personal Data
Customer acting as the 'processor' with regard to Customer Personal Data for which its End Client is the data controller
Customer acting as the 'data exporter'
Customer acting as 'business' under US Data Protection Laws

Remesh where and to the extent the following applies:
Remesh acting as the 'processor' of Customer Personal Data
Remesh acting as the 'data importer'
Remesh as the 'service provider' under US Data Protection Laws

Such terms shall apply equally to substantially similar functions as defined under other Data Protection Laws.

For purposes of greater certainty, this Agreement applies to the scenarios described above solely to the extent applicable to the relationship between the parties. For example, (A) if Customer is acting solely as the controller of Customer Personal Data (and not as a processor of such data), then the provisions in this Agreement relating to Module 3 of the SCCs shall **not** apply; and (B) Conversely, if Customer is acting as a processor Customer Personal Data on behalf of its End Client, then the provisions of this Agreement relating to Module 3 of the SCCs shall apply to such relationship.

Now, the parties hereby agree as follows:

1. Definitions.

For purposes of this DPA the following definitions shall apply:

1.1. "**controller**," "**processor,**" "**process/processing/processed**," "**data exporter**," "**data importer**," "**business**," "**service provider,**" and "**data subject,**" shall have the meaning assigned to such terms in the applicable Data Protection Laws.

1.2. "**Customer**" means the 'customer' as defined and identified in the Agreement relating to the provision of Remesh Solutions.

1.3. "**Customer Personal Data**" means any Personal Data provided by or on behalf of Customer to Remesh or which is otherwise Processed by Remesh on behalf of Customer in connection with the Agreement.

1.4. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under this DPA, including without limitation GDPR and those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the US Data Protection Laws.

1.5. "**End Client**" means a third party that is an end client of Customer for whose benefit Customer uses the Solutions to the extent authorized in the Agreement.

1.6. "**EU Personal Data"** means the processing of Personal Data to which data protection legislation of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its processing by Remesh.

1.7. "**European Personal Data"** means EU Personal Data, UK Personal Data, and Swiss Personal Data.

1.8. **"FADP**" means the Swiss Federal Act on Data Protection.

1.9. "**GDPR**" means the 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, and repealing Directive 95/46/EC, including as implemented or adopted under the laws of the UK, as amended from time to time.

1.10. "**Personal Data**" means any information relating to an identified or identifiable natural person including 'personal data' and 'personal information' as such terms are defined in applicable Data Protection Laws.

1.11. "**Privacy Policy**" means Remesh's then current policy governing its use of Personal Data found at https://live.remesh.chat/privacy-policy.

1.12. "**Protected Area"** means:

1.12.1. in the case of EU Personal Data, the members states of the European Union and the European Economic Area and any country, territory, sector, or international organisation in respect of which an adequacy decision under Art.45 GDPR is in force;

1.12.2. in the case of UK Personal Data, the United Kingdom and any country, territory, sector, or international organisation in respect of which an adequacy decision under United Kingdom adequacy regulations is in force; and

1.12.3. in the case of Swiss Personal Data, any country, territory, sector, or international organisation which is recognised as adequate under the laws of Switzerland.

1.13. "**SCCs**" means:

1.13.1.1. in respect of EU Personal Data, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, including where Customer is acting as the controller the text from module two and where Customer is acting as a processor on behalf of its End Client the text from module three of such clauses and in each case with Remesh acting as a processor, and adopted as set out in Exhibit C ("**EU SCCs**");

1.13.1.2. in respect of Swiss Personal Data, the EU SCCs, provided that any references in the clauses to the GDPR shall refer to the FADP; the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses; and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP;

1.13.1.3. in respect of UK Personal Data, the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum so that: (I) the details of the parties in table 1 shall be as set out in Exhibit A (with no requirement for signature); (ii)for the purposes of table 2, the addendum shall be appended to the EU SCCs (including the selection of modules and disapplication of optional clauses as noted above) and Clause 4 and Exhibit C below select the option and timescales for clause 9; and (iii) the appendix information listed in table 3 is set out in Exhibits A and B hereto.

1.14. "**Security Breach**" has the meaning set forth in Section 8.1 hereof.

1.15. "**Solutions**" means the SaaS Software and Professional Services as further defined in the Agreement which are provided by Remesh to Customer pursuant to the Agreement.

1.16. "**Subprocessor**" means any subcontractor engaged by Remesh or its Affiliates to Process Customer Personal Data.

1.17. "**Swiss Personal Data**" means Personal Data to which the FADP was applicable prior to its processing by Remesh.

1.18. “UK Personal Data” means the processing of Personal Data to which data protection laws of the United Kingdom were applicable prior to its processing by Remesh.

1.19. “**US Data Protection Laws**” means any and all applicable state or federal laws or regulations within the United States relating to data privacy or data protection including any amendment, update, modification to, or re-enactment of such laws.

Other capitalized terms used herein that are not defined herein shall have the meaning assigned to them in the Agreement.

2. Processing of Personal Data

2.1. This DPA shall apply where (i) Remesh processes Customer Personal Data for Customer in its role acting as a data controller of its own Customer Personal Data; and/or (ii) Remesh processes Customer Personal Data for Customer in its role acting as a processor on behalf of its End Clients. Where Customer is acting as a processor, Customer is responsible for fulfilling the controller’s obligations under this DPA.

2.2. Customer hereby appoints and instructs Remesh to process Customer Personal Data in its provision of Solutions to Customer, in accordance with the requirements of Data Protection Laws and Customer’s documented instructions as described in the details of the processing set forth in Exhibit A. Remesh shall process Customer Personal Data solely for the following purposes: (in) processing in accordance with the Agreement; (ii) processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; and (iii) processing as otherwise required by Data Protection Laws, provided that Remesh shall inform Customer of such other legal requirement before processing, unless prohibited by Data Protection Laws. For the avoidance of doubt, Remesh may not sell Customer Personal Data to third parties.

2.3. Remesh will only process the minimum amount of Customer Personal Data necessary to perform the Solutions (“purpose limitation”), unless on further instructions from the Customer.

2.4. Customer’s instructions for the processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer specifically acknowledges that its use of the Solutions will not violate the rights of any data subject that has objected to or opted-out of processing, sales, or other disclosures of Personal Data, to the extent applicable under applicable Data Protection Laws.

2.5. Remesh shall treat Customer Personal Data as Confidential Information pursuant to the terms of the Agreement.

2.6. Remesh will process Customer Personal Data using pseudonymous or de-identified values whenever reasonably possible so that it can no longer be attributed to a Data Subject without the use of additional information.

2.7. Remesh shall ensure that all persons authorized to process Customer Personal Data as a Subprocessor of Remesh have committed themselves to confidentiality and comply with Section 3.1 herein.

3. Subprocessors

3.1. Remesh may engage Subprocessors to process Customer Personal Data in connection with provision of Solutions under the Agreement provided that (i) Remesh will comply with the requirements of the Agreement with regard to providing notification to Customer of such Subprocessors; (ii) to the extent applicable and except as otherwise expressly stated in the Agreement or the DPA, Remesh will impose materially the same obligations on any Subprocessor as are imposed on Remesh hereunder with regard to its processing activities; and (iii) Remesh will take reasonable steps to ensure that its Subprocessors implement appropriate technical and organizational measures designed to comply with this DPA and Data Protection Laws. Remesh will maintain a list of its then current Subprocessors as a link in its Privacy Policy. Customer may object in writing, to any Subprocessor that Customer reasonably believes does not meet the privacy and security standards and other requirements under the Agreement. Customer must provide its objection in writing within 15 days from receipt of the initial notice regarding use of a subcontractor from Remesh. If Customer objects in writing within such period, Remesh and Customer shall collaborate in good faith to satisfy Customer’s concerns provided that if such concerns cannot be reasonably satisfied in mutually agreed upon manner, Customer may terminate this affected Processing by prior written notice. Subject to Remesh’s compliance with this Section 3.1 and the terms of this DPA and the Agreement, Customer consents to Remesh’s use of Subprocessors for purposes of the SCCs.

3.2. Remesh shall be liable for the acts and omissions of its Subprocessors in connection with the processing of Customer Personal Data to the same extent Remesh would be liable if performing the Solutions of each Subprocessor directly under the terms of this DPA, except as otherwise expressly set forth in the Agreement.

4. Data exports from the European Union - SCCs

4.1. Customer acknowledges and agrees that Remesh may process, access, and store Customer Personal Data in the United States and the other locations set forth in Exhibit A (Details of Processing of Customer Personal Data) solely as necessary to provide the Solutions (as such terms are defined in the Agreement) (the "**Permitted Transfers**").

4.2. Remesh shall be permitted to transfer European Personal Data outside of the Protected Area for the Permitted Transfers, and the parties agree to comply with the obligations set out in the SCCs as though they were set out in full in this DPA, with Customer as the 'data exporter' and Remesh as the 'data importer', with the parties signature and dating of the Agreement being deemed to be the signature and dating of the SCCs and with the Annexes to the EU SCCs being as set out in Exhibits A and B of this DPA.

4.3. The parties agree that for the purposes the SCCs, Customer consents to Remesh's use of the Subprocessors in accordance with the provisions set out in the Agreement. The parties agree that any rights to audit required pursuant to the SCCs, to the maximum extent permitted by the Data Protection Laws, will be exercised in accordance with the audit provisions set forth in this DPA and the Agreement. As between Customer and Remesh, Remesh's total aggregate liability under this DPA and the SCCs shall be subject to the limitations of liability agreed upon in the Agreement. The parties agree that in the event of any conflict between this DPA and the SCCs, the SCCs shall prevail.

4.4. Remesh agrees to take such other reasonable and appropriate steps or implement other safeguards as required to remain compliant with the GDPR, including any requirements that may be adopted by the European Commission or a competent European data protection authority that apply to data transfers from the European Union subsequent to execution of this DPA or that causes a Permitted Transfer outside of the Protected Area to be unlawful. In the event that GDPR, FADP, or the SCCs are amended and Remesh is not able to reasonably comply with the requirements of such amendments, Remesh will promptly notify Customer and the parties will work in good faith to resolve the issues. If a resolution cannot be mutually agreed upon, Remesh will cease processing Customer European Personal Data as affected by such amendments and Customer will have the right to terminate the Agreement as it relates to such Personal Data.

4.5. Remesh shall notify Customer without undue delay and no later than 24 business hours of its receipt of any data access requests made by national authorities, unless this information conflicts with statutory law.

4.6. Remesh shall provide adequate guarantees for the lawful processing of European Personal Data in compliance with the GDPR and shall ensure that data subject have enforceable rights and effective corrective legal measures through any of the instruments provided in the GDPR.

5. Assistance

5.1. Promptly upon request, Remesh shall provide reasonable assistance as otherwise required under the Data Protection Laws to enable Customer to meet its obligations under Data Protection Laws and to demonstrate Remesh's compliance with Data Protection Laws.

5.2. Promptly upon request, Remesh shall make available to the Customer all the information and documents that are necessary and required to demonstrate compliance with the provisions of Data Protection Laws.

5.3. Without limiting the generality of the foregoing, where required by applicable Data Protection Laws, Remesh shall maintain a record of all processing activities carried out on behalf of Customer.

5.4. Upon Customer's request, Remesh will provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Solutions, to the extent Customer does not otherwise have access to the relevant information.

6. Legal Requests

6.1. Remesh shall implement and maintain a documented procedure for reviewing and responding to any request for access to or disclosure of Customer Personal Data by any competent governmental or public authority (including any law enforcement authority) or pursuant to any legal, regulatory, or administrative requirement, order, or similar request ("**Personal Data Request**"). Such procedure shall, at a minimum, require that (i) Remesh, to the extent permitted by applicable law, promptly provide advance written notice to Customer of such Personal Data Request; (ii) cooperate with Customer in responding to such Personal Data Request; (iii) review the Personal Data Request to determine its validity and reject any request that is not valid, legally binding, or lawful; (iv) make reasonable efforts to direct the relevant authority to request the Customer Personal Data directly from Customer; (v) use reasonable efforts to assist Customer in its efforts to oppose or challenge such request and if Remesh is prohibited under applicable law from notifying Customer of such request, to the extent required under the Data Protection Laws, use reasonable efforts to oppose or challenge such request in a court of competent jurisdiction and seek permission to allow Customer to intervene in the proceedings.

6.2. If such Personal Data Request prevents Customer from complying with the SCCs, Remesh will promptly inform Customer of its inability to comply.

6.3. If disclosure of Customer Personal Data is legally required (following challenge of such request as required hereunder), Remesh will only disclose Customer Personal Data that is directly relevant and required for the response, and then disclose only the minimum amount necessary to comply with the request, and to the fullest extent permitted by applicable law, remove any information prior to disclosure that would directly allow the identity of the data subject to be identified from the data disclosed.

6.4. Remesh shall maintain a written record of all Personal Data Requests and, to the extent permitted by applicable law, Remesh shall make aggregated information from such records available to Customer upon request.

7. Data Security

7.1. 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, Remesh shall implement and maintain appropriate technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Personal Data. Remesh shall regularly monitor compliance with such measures and evaluate whether additional safeguards should be implemented.

7.2. Without limiting the foregoing, Remesh's security safeguards shall meet or exceed any requirements under Data Protection Laws and shall comply with the Security Controls set forth in Exhibit B hereto.

7.3. In the event Remesh obtains third-party certifications or audits of its security controls, upon Customer's written request at reasonable intervals (not to exceed one time per year), and subject to the confidentiality obligations set forth in the Agreements, Remesh shall make available to Customer a summary of any reports or findings of such audits. In addition, Customer shall have any audit rights specified in the Agreements.

8. Security Breaches

8.1. In the event of unauthorized access to, disclosure or acquisition of Customer Personal Data while in the possession of Remesh (a "**Security Breach**"), Remesh shall notify the Customer without undue delay (and no later than 48 hours of becoming aware of such Security Breach or such time earlier as specified in the Agreement as applicable). The Security Breach notice shall be provided via email to Customer's designated security person as noticed to Remesh via email to privacy@remesh.org.

8.2. The foregoing notification shall, where possible, contain a description of the nature of the Security Breach, in particular the categories and approximate number of Data Subjects affected, and the likely consequences of such Security Breach. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Remesh shall reasonably cooperate with the Customer in the investigation of a Security Breach, and in the identification, prevention, and mitigation of the effects of such Security Breach, as well as any other relevant information including for the purpose of communications with government authorities.

9. Exercise of Rights by Data Subjects

9.1. Remesh shall, to the extent legally permitted and to the extent that the data subject can be identified as a data subject of Customer, promptly (within five (5) business days unless otherwise specified in the Agreement) notify Customer if Remesh receives a request from a data subject to exercise the Data Subject's rights under Data Protection Laws, which may include the right of access, right to rectification, restriction of processing, deletion/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, a "**Data Subject Request**"). Unless otherwise required by applicable law, Remesh will not respond directly to a Data Subject Request. Taking into account the nature of the processing, Remesh shall reasonably assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a verified Data Subject Request under Data Protection Laws.

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

10. Return or destruction of Personal Data

10.1. Customer may delete its Customer Personal Data from the Solution SaaS Platform at any time, and Customer is responsible for such deletion. In addition, upon Customer's request, Remesh shall securely delete or destroy (and make available to Customer for download) any Customer Personal Data Processed on behalf of Customer. Notwithstanding the foregoing, at Customer's election, Remesh shall return (or make available for download) any Customer Personal Data processed on behalf of Customer.

10.2. Notwithstanding the above, Remesh's deletion and return obligations shall not apply where the Remesh is required to maintain Personal Data under Data Protection Laws.

11. Limitation of Liability

11.1. Each party's liability, taken together in the aggregate, arising out of or related to this DPA (including the SCCs), whether in contract, tort, or under any other theory of liability, is subject to any limitation of liability contained in the Agreement, and any reference in the Agreements to the liability of a party means the aggregate liability of that party under the Agreement and this DPA (including the SCCs) taken together.

The parties' authorized signatories have duly executed this DPA:

CUSTOMER: ____________________

Signature:______________________________

Print Name: ____________________________

Title: _________________________________

Date: _________________________________

Email: _____________________________

Email for Notices under this DPA:__________

REMESH INC.

Signature:______________________________

Print Name: ____________________________

Title: _________________________________

Date: _________________________________

Email: ___________________________

Email for Notices under this DPA:__________

Exhibit A
Details of the Processing of Customer Personal Data

This Exhibit A includes certain details of the processing of Customer Personal Data as may be required by Data Protection Laws, including without limitation Article 28(3) of the GDPR.

Data Exporter:

The data exporter is the business identified as the Customer in the DPA, which desires to avail itself of the Solutions provided by the data importer.

Contact Details: As set out in the Agreement or as otherwise notified in writing by Customer

Data Importer:

The data importer is Remesh as identified in the DPA, a U.S. company that provides customers the ability to have on-line conversations using Software as a Service (SaaS) and guided by real people who provide participant feedback.

Contact Details: Ross Coudeyras, DPO email: privacy@remesh.org or as otherwise notified in writing by Remesh.

Data Subjects:

The Personal Data transferred may concern the following categories of data subjects:

- Customer (and their End Clients as applicable) and their respective affiliates and their respective employees and representatives who use the Remesh Solutions to run and observe the research Conversations (collectively as "Customer Users and Observers").
- Moderators leading the research Conversations.
- Participants (either externally sourced third parties or employees of Customer or its End Clients) serving as the respondents to the research Conversations who provide feedback to the research questions.

Categories of Personal Data:

The Personal Data transferred may concern the following categories of Personal Data:

- Moderators: may provide business contact details including first and last name, business email, employer, job title, and at their option, photos/images.
- Customer Users and Observers: may provide business contact details including first and last name, business email, employer, and job title.
- Participants: may provide demographic information such as gender, race, ethnicity, religion, health, sexual orientation, age range, income range, buying preferences, employment related information, other similar information, and general location. Participants access the Remesh Platform through an anonymous weblink, and there is no name, email, or other identifier attached to such Personal Data. However, the Solution allows the Moderator to request identifying Personal Data from Participants, but that is not a recommended use of the Solution. In addition, a Participant may voluntarily provide Personal Data which is not requested by the Moderator.
- OPTIONAL USE: Customers who opt-in may choose to provide Customer-provided Participant lists which include email addresses for such Participants. This data is maintained in a separate file and cannot be cross-correlated with the Conversation Personal Data on an individual basis.

IP Addresses: For all individuals who access the Solution SaaS Platform, the system logs captured IP addresses, which can provide geo-location. This information is stored temporarily (auto deleted every 30 days). Such logs are segregated from the SaaS Platform data but may be accessed for fraud detection or similar circumstances by Remesh need-to-know staff.

Special categories of Personal Data:

The Personal Data transferred concern the following special categories of Personal Data:

Participants: These individuals may provide 'special category' personal information or 'sensitive' personal data, such as information regarding their race, religion, ethnicity, mental or physical health, sexual orientation, or citizenship or immigration status. This data is held in pseudonymised form to the extent reasonably possible as described above, and it is only used to provide the Solutions ("Limit the Use of My Sensitive Personal Information").

Purpose of Processing Operations:

Provision of the Solutions to the Customer as described in the Agreement.

Nature of Processing Operations:

The Personal Data transferred will be subject to the processing activities described in the Agreement in relation to the Remesh's provision of Solutions to the Customer. The Solution Platform is hosted in the United States. Customer understands and agrees that Remesh is entitled to (i) transfer, access, process, and store Personal Data to/in the United States and globally to Remesh's personnel for purposes of providing support and (ii) transfer to and allow processing by Subprocessors to perform translation, research, and sample Professional Services for the Solutions all as defined in the Agreement. In addition, the parties understand and agree that Customer Personal Data may be processed and transferred to (i) any country where Customer or the Customer Users and Observers are located, and (ii) to any country where the Participants and/or Moderators in a Conversation are located solely as necessary to provide the Solutions.

Subprocessors are identified in the Remesh Privacy Policy found at https://live.remesh.chat/privacy-policy. Remesh may update the Subprocessor list from time to time in accordance with the process described in the Agreement.

Frequency of the Transfers:
Continuously during the provision and use of the Solutions and the Conversation.

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

For the duration of the Agreement and until the Customer requests deletion. Customer is responsible for the deletion of Customer Personal Data stored on the Solution SaaS Platform provided that if Customer requests deletion in writing, Remesh will delete such Customer Personal Data.

Exhibit B

Remesh Security Controls

This Exhibit describes Remesh's security program and provides a description of the technical and organizational measures implemented by Remesh as the processor under the Agreement in Processing Customer Personal Data. Unless otherwise defined herein, capitalized terms have the meaning set forth in the Agreement.

1. Security Program

Remesh shall maintain, monitor, update, and enforce a comprehensive written data security program utilizing generally accepted industry best practices, which includes the following elements:

- Assigns sufficient resources and a Data Protection Officer responsible for overseeing the program;
- Establishes reasonable organizational, administrative, technical, and physical safeguards designed to protect the security, integrity, confidentiality, availability, and privacy of Personal Data, including protections against anticipated threats and hazards and security breaches;
- Establishes security principles of segregation of duties and least privilege with respect to Personal Data;
- Establishes appropriate technical measures designed to protect against the unauthorised or unlawful processing of the Customer Personal Data and against accidental loss or destruction of, or damage;
- Establishes data retention policies for reports, logs, audit trails, and other documentation that provides evidence of data security, systems, and audit processes and procedures;
- Establishes policies documenting the consequences for violations of data security policies;
- Establishes policies for security and privacy training; and
- Requires deploying security patches to all systems that Process Personal Data as necessary to comply with the Agreement and Data Protection Laws.

Remesh shall regularly review and update its security program and technical measures taking into account the available technology and the cost of implementing the specific measures designed to ensure a level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

2. Technical Measures

The Remesh security program, at a minimum, will implement the technical measures specified in this Exhibit.

2.1 Access Control to Premises and Facilities

Remesh uses a third party cloud provider to host the Remesh SaaS Platform. Remesh shall require its cloud hosting provider to implement measures to prevent unauthorized physical access to the cloud hosting premises and facilities holding Personal Data. Such measures include:

- Access control system
- ID reader, magnetic card, chip card
- Issuing of keys
- Door locking (electric door openers, etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitoring
- Logging of facility exits/entries

2.2 System Access Control

Remesh has implemented measures designed to prevent unauthorized access to its SaaS Platform. These include the following technical and organizational measures for user identification and authentication:

- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators
- Background checks on employees and contractors
- Personal/individual user log-in when logging into the system or company network (no shared credentials)
- Restricted access for guest users or anonymous accounts

- Compulsory use of multi-factor authentication (MFA)
- Host and network IDS/IPS
- Protection against malware/viruses – maintain up-to-date definitions and security patches for all systems and software to prevent against commonly known threats where feasible
- Password procedures (high complexity based on NIST standards) for Remesh staff:

Area	**Guideline**
Minimum password length	12 characters
Password complexity	Contains characters from at least three of the five categories: English uppercase; English lowercase; base ten (10) digits (i.e., 0-9); non-alphanumeric (i.e., !, $, #, %); and Unicode characters (i.e., ‡, €, Ÿ, or ƒ)
Maximum password lifetime	At most 90 days
Minimum password history	Where possible, passwords must not be reused for the past 365 days
Protection in transit	Mandatory - passwords must be encrypted in transit
Protection in storage	Mandatory - passwords must be hashed using an approved hash algorithm (see Disclosure Control table below)

2.3 Data Access Control

Remesh has implemented measures to prevent authorized users of its systems from accessing data beyond their authorized access rights. Such measures include:

- Differentiated access rights
- Access rights defined according to duties, including least privilege and need-to-know
- Automated log of user access via IT systems
- Quarterly review of access permissions, including approval routines

2.4. Disclosure Control

Remesh has implemented measures designed to prevent unauthorized access, alteration, or removal of data during transfer, and to ensure that all transfers are secure and are logged. Such measures include:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256). The permitted encryption procedures are selected according to current technological standards, examples below.

Domain	Key Type	Algorithm	Key Length
Web Certificate	Digital Signature	DSA or RSA PCKS#1	2048 bit
Web Cipher	Encryption	AES	256 bit
Password	Hash	Bcrypt, PBKDF2, or scrypt, ECDH	256 bit+10K Stretch
Laptop HDD	Encryption	AES	128 or 256 bit

- Prohibition of storing or processing of confidential information via portable media without adequate protection (e.g., encryption at rest)
- Creating an audit trail of data transfers where feasible
- Sufficient capacity of IT systems and equipment

2.5 Input Control

Remesh has implemented measures to ensure data management and maintenance is logged, provide an audit trail of whether data have been entered, changed, or removed (deleted) and specify by whom it must be maintained. Such measures include:

- Logging user activities on IT systems where feasible
- Change control process and procedures
- Comprehensive Software Development Life Cycle (SDLC) program

2.6 Job Control

Remesh has implemented measures to ensure that Personal Data is processed strictly in compliance with Customer's instructions. Such measures include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

2.7 Availability Control

Remesh has implemented measures designed to ensure that data processed on the SaaS Platform is protected against accidental destruction or loss. These measures include:

- Backup procedures and testing
- Incident response, disaster recovery, and business continuity management are reviewed and tested at least annually
- Offsite storage in the US-based multi-region of Remesh's third party cloud hosting provider
- Firewall systems (i.e., web application firewall)
- Monitoring of systems and infrastructure
- The ability to restore the availability and access to Personal Data in a timely manner in the event of an incident

2.8 Segregation Control

Remesh has implemented measures to allow data collected for different purposes to be processed separately. These include:

- Restriction of access to data stored for different purposes according to staff duties
- Segregation of business IT systems
- Segregation of IT testing and production environments

2.9 Pseudonymization

Remesh will Process Personal Data on the SaaS Platform using pseudonymous or de-identified values whenever reasonably possible as further described in the Processing Details of the DPA.

3. Measures to Validate Controls

Remesh has implemented a process for regularly evaluating, testing, and assessing current-state risk assessment of the security controls in place and identifying the gaps between current and mandated requirements.

- Remesh will maintain a SOC 2 Type II yearly certification and will require its cloud hosting provider for the SaaS Platform to maintain appropriate industry certifications (e.g., SSAE 18, SOC I, II, and III, ISO, or other certifications) during the term of the Agreement. Remesh's Subprocessors (but excluding Third Party Services providers (i.e., for Moderators and Sample Professional Services Vendors)) will have either a SOC, ISO, or a similar industry accepted certification.
- Periodic (minimum yearly) vulnerability and penetration testing by trusted third-party vendor
- Remesh shall have standards and procedures in place to address its security configuration, operation, and management that includes:
  - Security controls required for each of its system
  - Identification and patching of security vulnerabilities

4. Training

Remesh has implemented measures to provide privacy, data Processing, data protection, data security, encryption, and confidentiality awareness training annually to all individuals authorized by Remesh to Process Personal Data. Training shall occur before such individuals Process Personal Data, and such individuals shall repeat such training annually.

5. Data Destruction

Remesh has implemented measures governing the destruction and disposal of Personal Data. Upon Customer request, Remesh securely disposes of Personal Data and provides written confirmation of such destruction. Remesh reserves the right to maintain Personal Data to the extent retention is required for Remesh to comply with Data Protection Laws or as strictly necessary for Remesh's record keeping purposes in the ordinary course.

6. Security Reviews

Remesh shall reasonably cooperate with Customer, its designees and government, regulatory, and supervisory authorities, in connection with requests for information regarding Remesh's Processing of Customer Personal Data and any audit request to the extent required by Data Protection Laws. With respect to its third-party cloud hosting provider, Remesh shall use reasonable efforts to coordinate any such compliance obligations. Remesh shall respond to any Customer self-assessment security compliance reviews (including inspections and reviews for privacy, data Processing, data protection, data security, encryption, or confidentiality-related compliance). Upon request, and where possible in lieu of a physical audit requirement, Remesh will provide Customer a copy of its and its current cloud provider's industry certifications maintained in accordance with Section 3 herein.

Exhibit C
Standard Contract Clauses

EU SCCs

Where the parties rely on the EU SCCs, the parties acknowledge that these are adopted as follows:

- Customer is the Controller and/or Processor (as applicable and as described in the DPA) and Remesh is the Processor;
- All footnotes and explanatory notes in the EU SCCs are deleted;
- Clause 7 (Docking) shall be excluded;
- In respect of Clause 9 (sub-processors), Option 2 general written authorization applies, and the minimum time period for the data importer to specifically inform the data exporter in writing of any intended changes to that list in accordance with Clause 9 shall be fifteen (15) days unless a shorter time period is set forth in the Agreement;
- The “OPTION” in Clause 11(a) shall not apply and the wording in square brackets in that Clause shall be deleted;
- In respect of Clause 13(a) (supervision), the following wording shall apply: 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 as determined in accordance with GDPR;
- In respect of Clause 17 (governing law), Option 1 shall apply and the Member State governing law shall be the law of the Member State(s) in which the Customer that is the data exporter is located;
- In respect of Clause 18 (choice of forum and jurisdiction), the relevant courts shall be the courts of the Member State(s) in which the Customer that is the data exporter is located; and
- Exhibits A and Exhibit B of this DPA shall apply to Annexes I and II of the EU SCCs, respectively.