DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**Agreement**") and the changes to the Principal Agreement implemented by the Agreement, shall come into effect on 1 November 2019 ("**Effective Date**").

BETWEEN

you, hereafter referred to as "**Controller"**,

and

Meetio Inc., having its registered office at 700 SW Fifth Avenue, Portland, OR 97204 USA if the Controller is located in North or South America or Australia and **Meetio AB**, established and existing under the laws of Sweden, having its registered office at Eric Perssons väg 21, 217 62 Malmö, Sweden if the Controller is located in Europe, Middle East, Asia or Africa (Each, **"Meetio"**) hereinafter referred to as: "**Processor**".

RECITALS

(A) The Controller has entered into an End User License Agreement (the "**Principal Agreement**") with the Controller pursuant to which Processor will provide certain Services to Controller.

(B) To the extent that the provision of such Services involves the processing of personal data, the parties have agreed to enter into this Agreement for the purposes of ensuring compliance with the applicable Data Protection Laws.

THEREFORE, parties have agreed as follows:

DATA PROCESSING TERMS

1. DEFINITIONS

1.1 Terms such as "process/processing", "data subject", "data processor, "data controller", "personal data", "data breach", "data protection impact assessment", etc., shall have the same meaning ascribed to them in the Data Protection Laws;

1.2 "**Authorised Subprocessors**" means (a) those Subprocessors set out in Annex 2 (*Authorised Subprocessors*); and (b) any additional Subprocessors consented to in writing by the Controller in accordance with section 5.1;

1.3 "**Data Protection Laws**" means in relation to any Personal Data which is Processed in the performance of the Principle Agreement the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and all local implementing or supplementing laws thereto and any other applicable data protection or privacy laws;

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

1.5 "**Personal Data**" means the data described in Annex 1 (*Details of Processing of Personal Data*) and any other personal data processed by Processor or any Processor Affiliate on behalf of the Controller pursuant to or in connection with the Principal Agreement;

1.6 "**Services**" means the services described in the Principal Agreement;

1.7 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.8 "**Subprocessor**" means any data processor (including any third party and any Processor Affiliate) appointed by Processor to process personal data on behalf of the Controller;

1.9 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

2. PROCESSING OF THE PERSONAL DATA

2.1 Processor shall only process the types of Personal Data relating to the categories of data subjects for the purposes of the Principal Agreement and for the specific purposes in each case as set out in Annex 1 (*Details of Processing of Personal Data*) to this Agreement and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with the Controller's documented instructions (whether in the Principal Agreement or otherwise) unless processing is required by EU or Member State law to which Processor is subject, in which case Processor shall to the extent permitted by such law inform the Controller of that legal requirement before processing that Personal Data.

2.2 For the purposes set out in section 2.1. above, the Controller hereby instructs Processor to transfer Personal Data to the recipients in the countries listed in Annex 3 (*Authorised Transfers of Personal Data*) always provided that Processor shall comply with section 5 (*Subprocessing*) and 11 (*International Transfers of Personal Data*).

2.3 Parties agree that this Agreement amends and replaces: (i) the provisions in the Principal Agreement that relate expressly to the parties' use of Personal Data, including any specific data protection clauses and data protection schedules in engagement letters; and (ii) any other provisions in the Agreement that conflict with the terms of this Agreement.

3. PROCESSOR PERSONNEL

3.1 Without prejudice to any existing contractual arrangements between the parties, Processor guarantees that it shall treat all Personal Data as strictly confidential and that it shall inform all its employees, agents, contractors and/or Authorized Subprocessors engaged in processing the Personal Data of the confidential nature of such Personal Data. Processor shall take reasonable steps to ensure the reliability of any employee, agent, contractor and/or Authorized Subprocessor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those persons or parties who need to access the relevant Personal Data, as strictly necessary for the purposes set out in section 2.1 above in the context of that person's or party's duties to Processor.

3.2 Processor shall ensure that all such persons or parties involved in the processing of Personal Data:

3.2.1 have undertaken appropriate training in relation to the Data Protection Laws;

3.2.2 are subject to confidentiality undertakings (of which a copy shall be provided upon Controller's request); and

3.2.3 are subject to user authentication and log on processes when accessing the Personal Data.

4. SECURITY

4.1 Without prejudice to any other security standards agreed upon by the parties, Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk and shall take all measures required pursuant to article 32 GDPR. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. The technical and organisational measures shall include in any case reasonable measures:

4.1.1 to ensure that the Personal Data can be accessed only by authorized parties for the purposes set forth in Annex 1 (*Details of Processing of Personal Data*) to this Agreement;

4.1.2 to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

4.1.3 to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide Services to the Controller.

4.2 The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Processor will therefore evaluate the technical and organisational measures as implemented in accordance with this section on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with Data Protection Laws.

4.3 Controller may provide written notice to Processor if in the reasonable opinion of Controller the technical and organisational measures set out in this section need to be changed to take account of a change of Data Protection Laws and Processor shall implement such changes at no additional cost to Controller. Such written notice shall include a description of the change of law and details of the required changes.

5. SUBPROCESSING

5.1 Subject to section 5.3, Processor shall not engage any data processors to process Personal Data other than with the prior written consent of the Controller, which the Controller may refuse in its absolute discretion.

5.2 With respect to each Subprocessor, Processor shall:

5.2.1 provide the Controller with full details of the processing to be undertaken by the each Subprocessor;

5.2.2 carry out adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Agreement including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of Data Protection Laws and this Agreement;

5.2.3 include terms in the contract between Processor and each Subprocessor which are the same as or equivalent to those set out in this Agreement, and shall supervise compliance thereof. Upon request, Processor shall provide a copy of its agreements with Subprocessors to the Controller for its review;

5.2.4 insofar as that contract involves the transfer of Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Controller into the contract between Processor and each Subprocessor to ensure the adequate protection of the transferred Personal Data, or such other arrangement as the Controller may approve as providing an adequate protection in respect of the processing of Personal Data in such third country(ies); and

5.2.5 remain fully liable to the Controller for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of any Personal Data.

5.3 As at the Effective Date, the Controller hereby authorises Processor to engage those Subprocessors set out in Annex 2 (*Authorised Subprocessors*).

6. DATA SUBJECT RIGHTS

6.1 Processor shall promptly, and in any case within five (5) working days, notify the Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of that request.

6.2 Processor shall co-operate as requested by the Controller to enable the Controller to comply with any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or this Agreement, which shall include:

6.2.1 the provision of all information requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a data subject;

6.2.2 where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and

6.2.3 implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

7. INCIDENT MANAGEMENT

7.1 Processor shall notify the Controller immediately, and in any case within twenty-four (24) hours upon becoming aware of or reasonably suspecting a data breach, providing the Controller with sufficient information which allows the Controller to meet any obligations to report a data breach under the Data Protection Laws. Such notification shall as a minimum:

7.1.1 describe the nature of the data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

7.1.2 communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 describe the likely consequences of the data breach; and

7.1.4 describe the measures taken or proposed to be taken to address the data breach.

7.2 Processor shall fully co-operate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each data breach, in order to enable the Controller to *(i)* perform a thorough investigation into the data breach, *(ii)* formulate a correct response and to take suitable further steps in respect of the data breach in order to meet any requirement under the Data Protection Laws.

7.3 The parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which Processor is subject, in which case Processor shall to the extent permitted by such law inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the data breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1 Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 GDPR and with any prior consultations to any Supervisory Authority of the Controller or any of its affiliates which are required under Article 36 GDPR, in each case in relation to processing of Personal Data by Processor on behalf of the Controller and taking into account the nature of the processing and information available to Processor.

9. DELETION OR RETURN OF CONTROLLER PERSONAL DATA

9.1 Processor shall promptly and in any event within 90 (ninety) calendar days of the earlier of: *(i)* cessation of processing of Personal Data by Processor; or *(ii)* termination of the Principal Agreement, at the choice of the Controller either:

9.1.1 return a complete copy of all Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely wipe all other copies of Personal Data processed by Processor or any Authorised Subprocessor; or

9.1.2 securely wipe all copies of Personal Data processed by Processor or any Authorised Subprocessor,

and in each case provide written certification to the Controller that it has complied fully with this section 9.

10. AUDIT RIGHTS

10.1 Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement and allow for and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the processing of Personal Data takes place. Processor shall permit the Controller or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of Data Protection Laws and this Agreement are being complied with. Processor shall provide full co-operation to the Controller in respect of any such audit and shall at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Agreement. Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section infringes the GDPR or other EU or Member State data protection provisions.

11. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

11.1 Processor shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Subprocessor to (permanently or temporarily) process the Personal Data in a country outside of the European Economic Area without an adequate level of protection, other than in respect of those recipients in such countries listed in Annex 3 (*Authorised Transfers of Personal Data*), unless authorised in writing by the Controller in advance.

11.2 When requested by the Controller, Processor shall promptly enter into (or procure that any relevant Subprocessor of Processor enters into) an agreement with the Controller including or on such clause as adopted by the European Commission and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the European Economic Area without an adequate level of protection.

12. INDEMNITY

12.1 Notwithstanding any contrary provisions in the Principal Agreement, Processor indemnifies the Controller and holds the Controller harmless against all claims, actions, third party or Supervisory Authority claims, losses, damages and expenses incurred by the Controller and arising directly or indirectly out of or in connection with a breach of this Agreement by the Processor.

12.2 The indemnity obligations set out in this clause 12 shall not be subject to any limitations of liability as set out in this agreement and/or the Principal Agreement.

12.3 Controller is not liable for any damage or cost, either by contract or tort, towards the Processor or any of its Authorized Subprocessors under this Agreement, except in case of gross negligence or wilful misconduct.

13. INTELLECTUAL PROPERTY

13.1 The provision of Personal Data and/or any other data by the Controller to the Processor shall not constitute a grant of license or a transfer of rights further than has been explicitly granted in writing by the Controller to the Processor.

14. MISCELLANEOUS

14.1 Subject to section 14.2, the parties agree that this Agreement and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry or termination of all service contracts entered into by Processor with the Controller pursuant to the Principal Agreement, whichever is later.

14.2 Any obligation imposed on Processor under this Agreement in relation to the processing of Personal Data shall survive any termination or expiration of this Agreement.

14.3 With regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this Agreement shall prevail with regard to the parties' data protection obligations for Personal Data. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.4 Compliance by Processor with the provisions of this Agreement will be at no additional cost to the Controller.

14.5 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement 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.

14.6 This Agreement is governed by the laws of Sweden. Any disputes arising out or in connection with this Agreement shall be brought exclusively before the competent court of Stockholm.

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex 1 includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Personal Data

Meetio provides products and services for meetings and meeting related tasks. The subject matter of processing of Personal Data is the provision of the services to the Controller that involves processing of Personal Data. Personal Data may be processed for the duration of the Agreement or otherwise by the parties agreed upon duration.

The nature and purpose of the processing of Personal Data

In order to provide the services required by the Processor to fulfil its obligations towards the Controller, the Processor may store, access or in other ways process Personal Data on behalf of the Controller. Anonymized data from which natural persons cannot be identified, derived from Personal Data, may be processed and used for providing anonymous meeting statistics and insights to third parties.

The types of Personal Data to be processed

For the purpose of sales, marketing and support: Contact information (name, email, phone number, employer, job position, country of residence). When contacted directly through our website (contact form, chat tool) also location data, IP-address, website usage data, device operating system, browser version and any other Personal Data that the Natural Person contacting us provides in free text.

For the purpose of providing the services specified in the Agreement: Contact information, system usage data, calendar and meeting data including name and email of meeting attendees, user initiated system actions (like check-in, end early and booking of meetings) and other Personal Data submitted, stored, sent or received by end users through the services.

The categories of data subject to whom the Personal Data relates

Controller's employees and their contacts, including end users given access to the services by the Controller. Data Subjects may also be individual Natural Persons communicating or in other ways transferring Personal Data to the Controller, its end users or the Processor.

The obligations and rights of Controller additional to the obligations and rights set out in the Agreement

This Agreement is the Controllers complete and final instructions to the Processor in relation to Personal Data and the Processing thereof. Any additional instructions outside of the scope of this Agreement requires prior written agreement between the parties. The Controller shall without undue delay inform the Processor of any errors or irregularities related to statutory provisions on the Processing of Personal Data.

ANNEX 2: AUTHORISED SUBPROCESSORS

Meetio uses a number of Subprocessors to assist in providing the Services. These Subprocessors provide hosting and storage, content delivery, communication tools and other tools to assist in customer relation management, support, incident tracking, diagnostics and resolution services.

Following is a list of Authorized Subprocessors:

- Amazon Web Services Inc.
- Atlassian Inc.
- GetAccept Inc.
- Google LLC.
- Hubspot Inc.
- Microsoft Ireland Operations Inc.
- OnlineCity ApS (Gateway API)
- Sendgrid Inc.
- Stripe Inc.
- Tawk.to Inc.
- Zenleads Inc.
- Meetio AB
- Meetio Inc.
- Any other wholly-owned Meetio Holding AB subsidiary organizations

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

For the purpose of providing the services specified in the Agreement:

Third Party Service	Entity location	Processing purpose
Amazon Web Services Inc.	Germany	Data and Services hosting
Amazon Web Services Inc.	Ireland	Transactional emails
Google Ireland Ltd.	Ireland	Google Analytics
Google LLC*	USA	Calendar integration, only applicable if Controller will integrate with Gsuite (Google Calendar) as calendar system. Actual entity location is specific to, and controlled by, the Controller.
Meetio AB	Sweden	Processor
Meetio Inc.	USA	Processor
Microsoft Inc.	Ireland	Calendar integration, only applicable if Controller will integrate with Microsoft Office365 or Microsoft Exchange as calendar system. Actual entity location is specific to, and controlled by, the Controller.
OnlineCity ApS	Denmark	SMS and content delivery integration for some services (opt-in)
Sendgrid Inc.*	USA	Content delivery and notifications

* Privacy Shield certified sub processor. See details at https://www.privacyshield.gov

For the purpose of sales, marketing and support:

Third Party Service	Entity location	Processing purpose
Atlassian Inc.*	Ireland, USA	Customer relation management, support and issue tracking
GetAccept Inc.*	Sweden, USA	E-signature tool
Google LLC	Ireland	Google Analytics
Hubspot Inc.*	USA	Customer relation management
Microsoft Inc.	Ireland	Customer relation management
Sendgrid Inc.*	USA	Content delivery, Customer relation management
Stripe Inc.*	USA	Online Payments
Tawk.to Inc.*	USA	Customer relation management and support
Zenleads Inc.	USA	Customer relation management
Meetio AB	Sweden	Processor
Meetio Inc.	USA	Processor

* Privacy Shield certified sub processor. See details at https://www.privacyshield.gov