DATA PROCESSING AGREEMENT

between

omos media GmbH
registered with the commercial register of the local court of Charlottenburg (Berlin) under HRB 193648 B and with business address at Lützowstraße 105/106, 10785 Berlin

– hereinafter "controller" and the "First Controller" –

and

Gemma Analytics GmbH
registered with the commercial register of the local court of Charlottenburg under HRB 215822 B and with business address at Chausseestraße 17, 10115 Berlin

– hereinafter "processor" and the "First Processor" –

– all controllers and processors hereinafter collectively the "Parties", each a "Party".

SECTION I

Clause 1 – Purpose and scope

1. The purpose of this Data Processing Agreement ("DPA") is to ensure compliance with Article 28(3) and (4) of 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.

2. The controllers and processors listed in Appendix I have agreed to the DPA in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.
3. The DPA applies to the processing of personal data as specified in Appendix II.
4. Appendices I to IV are an integral part of the DPA.
5. The DPA is without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.
6. The DPA does not by itself ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2 – Invariability of the Clauses

1. The Parties undertake not to modify the DPA, except for adding information to the Appendices or updating information in them.
2. This does not prevent the Parties from including the standard contractual clauses laid down in the DPA in a broader contract, or from adding other clauses or additional safeguards, provided that they do not directly or indirectly contradict the DPA or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

1. Where the DPA uses the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. The DPA shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. The DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 – Hierarchy

In the event of a contradiction between the DPA and the provisions of related agreements between the Parties existing at the time when the DPA is agreed or entered into thereafter, the DPA shall prevail.

Clause 5 – Docking clause

1. Any entity that is not a Party to the DPA may, with the agreement of all the Parties, accede to the DPA at any time as a controller or a processor by completing the Appendices and signing Appendix I.
2. Once the Appendices in (1) are completed and signed, the acceding entity shall be treated as a Party to the DPA and have the rights and obligations of a controller or a processor, in accordance with its designation in Appendix I.
3. The acceding entity shall have no rights or obligations resulting from the DPA from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Appendix II.

Clause 7 – Obligations of the Parties

7.1. Instructions

1. The processor shall process personal data only on appropriately documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
2. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Appendix II.

7.4. Security of processing

1. The processor shall at least implement the technical and organizational measures specified in Appendix III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
2. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

1. The Parties shall be able to demonstrate compliance with the DPA.

2. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with the DPA.
3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in the DPA and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by the DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
4. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
5. The Parties shall make the information referred to in the DPA, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

1. The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with the DPA to a sub-processor, without the controller's prior specific written authorization. The processor shall submit the request for specific authorization at least 5 days prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorization. The list of sub-processors authorized by the controller can be found in Appendix IV. The Parties shall keep Appendix IV up to date.
2. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with the DPA. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to the DPA and to Regulation (EU) 2016/679.
3. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
4. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfill its contractual obligations.
5. The processor shall agree a third party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

1. Any transfer of data to a third country or an international organization by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
2. The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2)

of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

1. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the controller.
2. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (1) and (2), the processor shall comply with the controller's instructions.
3. In addition to the processor's obligation to assist the controller pursuant to Clause 8(2), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
    1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
    4. the obligations in Article 32 Regulation (EU) 2016/679.
4. The Parties shall set out in Appendix III the appropriate technical and organizational measures by which the processor is required to assist the controller in the application of this Clause 8 as well as the scope and the extent of the assistance required.

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

1. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
2. in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
    1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    2. the likely consequences of the personal data breach;

3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

1. in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
2. the details of a contact point where more information concerning the personal data breach can be obtained;
3. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Appendix III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10 – Non-compliance with the DPA and termination

1. Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under the DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with the DPA or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with the DPA, for whatever reason.
2. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with the DPA if:
    1. the processing of personal data by the processor has been suspended by the controller pursuant to point (1) and if compliance with the DPA is not restored within a reasonable time and in any event within one month following suspension;
    2. the processor is in substantial or persistent breach of the DPA or its obligations under Regulation (EU) 2016/679;
    3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to the DPA or to Regulation (EU) 2016/679.

3. The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under the DPA where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (2), the controller insists on compliance with the instructions.
4. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with the DPA.

APPENDIX I: LIST OF PARTIES

First Controller

Place, Date

Controller
represented by:
Sebastian Berger
Head of E-Commerce & Development

First Processor

Place, Date

Processor
represented by:
Bijan Soltani
Managing Director
bijan.soltani@gemmaanalytics.com

First Processor's Data Protection Officer:
heyData GmbH
Schützenstr. 5
10117 Berlin
datenschutz@heydata.eu
www.heydata.eu

APPENDIX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Customers / interested parties / users of the controller
- Employees of the controller
- Suppliers of the controller

Categories of personal data processed

- Inventory data (e.g., names, addresses)
- Contact data (e.g., email, phone numbers)
- Content data (e.g., text entries, photographs, videos)
- Contract data (e.g., subject matter of contract, term)
- Payment data (e.g., bank details, payment history)
- Usage data (e.g., interests, websites visited, purchasing behavior, access times, log data)
- Meta/communication data (e.g., device IDs, IP addresses, location data)
- Employee master data (e.g., names, addresses, wage group, tax characteristics)
- Applicant data (e.g., names, contact details, qualifications, application documents)

Nature of the processing

- Review, temporary storage, and processing of personal data in the processor's local or project-specific development and test environments, insofar as necessary for analysis or technical implementation.
- Modeling, transformation, and quality assurance of data as part of development and implementation services (e.g., data modeling, pipeline logic, testing).
- Analysis and evaluation of data to identify business requirements, validate results, and prepare and create reports and dashboards.
- Configuration and implementation of development artifacts (e.g., ELT processes, dbt projects, Airflow DAGs, interfaces).
- Error analysis, debugging, and technical testing.
- Consulting and support services in the areas of data platforms, data models, and analytics architectures, insofar as the processing of personal data is required for such services.

Purpose(s) for which the personal data is processed on behalf of the controller

- Storage space (web hosting)
- Software as a service (computing capacity, databases, software)
- Telecommunication services (e-mails)
- Domain registration
- Software and design development/consulting or maintenance
- Server administration/ hardware maintenance
- Data analysis/ consulting services
- Advertising/ marketing

Duration of the processing

The duration of the data processing shall correspond with the respective Agreement between the Parties.

APPENDIX III: TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

Measure	Description
Access control	All entrances are adequately secured against unauthorized access, which means that: External doors are secured with manual locks; visitors are only allowed on the premises when accompanied by a member of staff; Third party personnel are carefully selected, especially for cleaning and maintenance tasks; When working in a home office: employees are instructed, if possible, to work in a room separate from living quarters.
Organizational data protection measures	Organizational measures: Regular training sessions are held on the subject of data protection. Regular sensitization of employees. A clean desk policy has been defined. The number of administrators is limited to the minimum necessary. General paper avoidance obligation. Personal data is regularly not printed out, but mainly processed digitally. Employees are also instructed to print only absolutely necessary data. Internal instruction to anonymize/pseudonymize personal data in the event of disclosure or after expiry of the statutory deletion period, if possible.
Transfer control	The aspects of the transfer of personal data are implemented by: encryption of data carriers and connections; WLAN encryption via WPA2 with strong password; During physical transport, suitable transport persons are carefully selected.
Data protection management	The following measures are intended to ensure that the organization meets the basic requirements of data protection law: Use of the heyData platform for data protection management;

	Appointment of the data protection officer heyData; Commitment of employees to data secrecy; Regular training of employees in data protection; Keeping an overview of processing activities (Art. 30 GDPR).
Incident Response Management	The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches: Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR); Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR vis-à-vis the data subjects (Art. 34 GDPR); Involvement of the Data Protection Officer in security incidents and data breaches.
Privacy-friendly default settings (Art. 25 (2) GDPR)	The following implemented measures take into account the requirements of the principles "Privacy by design" and "Privacy by default": Training of employees in "Privacy by design" and "Privacy by default"; No more personal data is collected than is necessary for the respective purpose.
Input control	The control of entries is carried out by: Logging of data entries, changes and deletions with manual or automatic control of the logs; access rights (both for users and administrators) are based on the requirements of the task and data protection law.
Order control	The awarding and monitoring of commissioned data processing operations result from the following: Selection of contractors under due diligence aspects; detailed regulations on the contractual relationship; Written instructions to the contractor or instructions in text form (e.g. by data processing agreement); Ensuring that data is destroyed after the order has been completed, e.g. by requesting appropriate confirmations; Confirmation from contractors that they commit their own employees to data secrecy (typically in the data processing agreement); Agreement on control and access or deletion rights.

APPENDIX IV: LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Name of Subcontractor	Address	Work to be performed	International Referral (if applicable)
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Germany	Cloud server (compute) for Airflow and Lightdash	None
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg	Managed PostgreSQL (RDS, Frankfurt region) and cloud computing (AWS Bedrock)	None
Langdock GmbH	Greifswalder Str. 212, 10405 Berlin, Germany	AI-powered workflows, document processing and general LLM usage (EU-hosted models only)	None
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Ireland	Cloud storage (Google Drive) and AI-powered meeting summaries (Gemini)	None
Anthropic, PBC	548 Market St, PMB 90375, San Francisco, CA 94104, USA	AI-powered software development and code generation (Claude)	USA, EU-SCCs
Mango Technologies, Inc. (dba ClickUp)	350 10th Ave, Suite 500, San Diego, CA 92101, USA	Project management and task tracking	USA, EU-SCCs
Notion Labs, Inc.	2300 Harrison Street, San Francisco, CA 94110, USA	Project management, task tracking, documentation and knowledge management	USA, EU-SCCs
Fireflies.AI Corp.	5424 Sunol Blvd, Ste 10-531, Pleasanton, CA 94566, USA	Meeting transcription and automated notes	USA, EU-SCCs