1. Preamble

This Data Processing Agreement governs the processing of personal data by the Processor on behalf of the Controller and is part of the Main Contract concluded between the Processor and the Controller. In the event of a conflict between the applicable agreement and the Data Processing Agreement, the Data Processing Agreement shall take precedence.

2. Definitions

Supervisory authority: An independent authority responsible for monitoring the application of data protection law.

Applicable privacy law: Refers to the European General Data Protection Regulation 2016/679 (GDPR) and the German Data Protection Act (BDSG).

Personal data: Information relating to a directly or indirectly identifiable natural person.

Sub-processors: A processor engaged by the Processor or its Affiliates to assist in the fulfilment of its obligations. Sub-processors may also include third parties or Affiliates of the Processor.

Affiliate: Any legal entity that either exercises control over the Processor, is controlled by the Processor, or is under common control with the Processor. "Control" in this context means the direct or indirect ownership of more than 50% of the voting shares of a legal entity or the ability to otherwise exercise significant influence over the business policies or decisions of the legal entity.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed by the (Sub-)Processor.

Instructions: Written instructions from the Controller to the Processor for the processing of personal data, specifying how personal data is to be processed, including the transfer, type of processing, duration, purpose, type of personal data and categories of Data Subjects. Instructions must comply with the applicable data protection laws, in particular the GDPR, and must be issued in writing or in a documented electronic format. Changes or additions to these instructions also require a documented form.

Controller, Data Subject, Processor, Processing: Terms with the meanings according to the GDPR.

3. Scope of application, subject matter, purpose and duration of processing

3.1 The Agreement shall apply to the collection, processing and deletion of all personal data that is the subject of the Service Agreement or that arises in the course of its implementation or becomes known to the Processor.

3.2 The subject matter and duration of the data processing as well as the scope, type and purpose of the intended processing of data are determined by the Service Agreement.

3.3 The following types or categories of data are subject to processing by the Processor:

- Professional contact or profile data (e.g. first and last name, e-mail address, position, department, location, as well as other required or voluntary profile information)
- Login data (e-mail address, password or data transmitted by the Controller via the SSO procedure (claims))

- Content (other personal data transmitted to the Processor by Users of the Controller or contained in Controller's data)
- Usage data (e.g. IP address, device properties, access times, user ID)

3.4 Categories of Data Subjects:

- Employees of the Controller
- Third parties who have been authorised by the Controller (e.g. Affiliates, service providers, consultants or agencies) or whose data is contained in the content.

4. Responsibility and Authority to Issue Instructions

4.1 The Parties shall ensure compliance with data protection provisions. The Parties understand and agree that with regard to the processing of personal data, the Client is the Controller and the Contractor is the Processor. The Controller may at any time request the disclosure, rectification, adaptation, erasure or restriction of the processing of the data.

4.2 In order to ensure the protection of the rights of the Data Subjects, the Processor shall provide the Controller with appropriate assistance, in particular by ensuring the implementation of appropriate Technical and Organisational Measures.

4.3 If a Data Subject contacts the Processor directly to assert a data subject right, the Processor shall forward this request to the Controller without delay.

4.4 The Processor may only process data within the framework of the Controller's instructions, unless the law of the Union or of the Member State to which the Processor is subject obliges the Processor to do otherwise (e.g. investigations by law enforcement or state security authorities); in which case the Processor shall notify the Controller of these legal requirements prior to processing, unless the law in question prohibits such notification on grounds of important public interest (Art. 28(3)(2)(a) GDPR).

4.5 The Processor must immediately inform the Controller if the Processor believes that an instruction violates data protection regulations. The Processor is authorised to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Controller. The persons authorised to issue instructions on the part of the Controller and the persons authorised to receive instructions on the part of the Processor, as well as the designated information channels, are specified in **Annex 1: List of Persons Authorised to Issue Instructions**. If no persons authorised to issue instructions are specified in Annex 1, the signatory of the Order Form is designated as the person authorised to issue instructions.

4.6 Any changes to the processing subject matter that constitute process changes must be jointly agreed and documented. The Processor may only provide information to third parties or the Data Subject with the prior express written consent of the Controller. The Processor shall not use the data for any other purposes and in particular shall not be authorised to disclose it to third parties. Copies and duplicates shall not be created without the knowledge of the Controller, except for necessary backups.

4.7 The Controller shall maintain a record of processing activities within the meaning of Art. 30(1) GDPR. The Processor shall provide the Controller with information to be included in the record at the Controller's request. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller in accordance with the requirements of Art. 30(2) GDPR.

4.8 The processing of data on behalf of the Controller shall take place exclusively within the territory of the European Union. Processing in a country outside the territory referred to in sentence 1 is only permitted if it is ensured that the level of protection guaranteed by the GDPR is not undermined, taking into account the requirements of Chapter V of the GDPR, and requires the prior consent of the Controller. Consent shall be deemed to have been granted if the Processor informs the Controller in advance of the measure with a notice period of 8 weeks, and the Controller does not object to it for a significant reason within this period. In the event of an objection, the Processor may terminate the contractual relationship with a notice period of 3 months. The basic requirements for the lawfulness of the processing shall remain unaffected.

4.9 The Processor shall ensure that natural persons under the Processor's authority who have access to data only process such data on the instructions of the Controller. The Controller shall grant the Processor consent to process the data outside the Processor's premises (e.g. working from home, mobile working) on the basis of the processing situation determined in **Annex 3: Technical and Organisational Measures**.

5. Compliance with Mandatory Legal Obligations by the Processor

5.1 The Processor shall ensure that the persons authorised to process the data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality and shall provide evidence of this to the Controller upon request. This also includes the information about the obligations to follow instructions and adhere to the purpose for which the data was collected that exist in this data processing relationship.

5.2 The Parties shall support each other in proving and documenting their accountability with regard to the principles of proper data processing, including the implementation of the necessary Technical and Organisational Measures (Art. 5(2), Art. 24(1) GDPR). The Processor shall provide the Controller with relevant information in this regard as required.

5.3 The Processor shall appoint a data protection officer who shall perform the relevant duties in accordance with the statutory provisions. The contact details of the data protection officer are heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu.

5.4 The Processor shall inform the Controller without undue delay of any inspections or measures carried out by the supervisory authorities or if a supervisory authority, within the scope of its competence, makes enquiries, conducts investigations or collects other information from the Processor, insofar as the Controller's data is affected by this measure.

6. Ensuring the Technical and Organisational Measures

6.1 The Parties agree to the specific technical and organisational security measures set out in **Annex 3: Technical and Organisational Measures** to this Agreement. The Annex is an integral part of this Agreement.

6.2 Technical and Organisational Measures are subject to technical progress. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the level of security of the measures specified in **Appendix 3: Technical and Organisational Measures** must not be compromised. Significant changes must be documented.

6.3 The Processor shall provide the Controller with all information necessary to demonstrate compliance with the provisions of this Agreement and the legal requirements. In particular, the Processor shall facilitate and support any audits/inspections conducted by the Controller or another auditor appointed by the Controller. Proof of the implementation of such measures, which do not solely pertain to the specific order, can also be provided by submitting a current certificate, reports from sufficiently qualified and independent bodies (e.g. auditors, independent data protection auditors), by compliance with approved codes of conduct pursuant to Art. 40 GDPR, certification pursuant to Art. 42 GDPR or an appropriate certification through an IT security or data protection audit (e.g. in accordance with BSI-Grundschutz, ISO 27001). The Processor undertakes to promptly inform the Controller about the exclusion of approved codes of conduct pursuant to Art. 41(4) GDPR, the revocation of a certification pursuant to Art. 42(7) and any other form of annulment or significant change to the aforementioned proofs.

6.4 The Controller may, with a notice period of 2 weeks, inspect the Processor's premises during regular business hours without disrupting operations, to verify the adequacy of the measures taken to comply with legal requirements or the technical and organisational requirements necessary for the execution of this contract. The obligation to provide timely notice does not apply if there is an important reason that necessitates an immediate audit.

6.5 The Processor shall also provide the Controller with all necessary information required for the audits mentioned in paragraph 4, as well as for an assessment of the impact of the planned processing activities on the protection of data (Data Protection Impact Assessment as per Art. 35 GDPR).

6.6 The Processor, in consultation with the Controller, must take all necessary measures to ensure the security of the data and the security of processing, particularly taking into account the state of the art, as well as to mitigate any potential adverse effects on Data Subjects.

6.7 The Processor shall support the Controller, taking into account the nature of the processing and the information available to them, in the context of a prior consultation as per Art. 36 GDPR.

6.8 The transfer of personal data to a third country (outside the EEA) may take place under the conditions specified in Articles 44 et seq. of the GDPR.

7. Notification of Breaches by the Processor

The Processor shall inform the Controller immediately in the event of significant disruptions to its operations, suspected violations of this agreement or statutory data protection regulations, breaches of such regulations, or other irregularities concerning the processing of the Controller's

data. This applies in particular with regard to the reporting obligation pursuant to Art. 33(2) GDPR, as well as to the corresponding obligations of the Controller pursuant to Art. 33 and Art. 34 GDPR. The Processor agrees to appropriately assist the Controller in fulfilling its obligations under Articles 33 and 34 GDPR where necessary. The Processor may only make notifications pursuant to Art. 33 or 34 GDPR on behalf of the Controller following prior instructions as per Section 4 of this agreement.

8. Deletion and Return of Data

8.1 Data carriers and data records provided shall remain the property of the Controller.

8.2 Upon completion of the contractually agreed services or earlier upon request by the Controller, but no later than upon termination of the service agreement, the Processor must destroy all documents, processing and usage results, as well as data sets (including any copies or reproductions thereof) that came into its possession in connection with the contractual relationship, in compliance with data protection regulations. A deletion log must be provided to the Controller upon request. Data sets are returned via provided export interfaces that enable the Controller to secure the data accordingly. The Controller shall ensure that the data records are backed up before the end of the service period if necessary, as later access is no longer possible due to implemented automated deletion processes. Backup copies (backups) are to be destroyed in accordance with data protection regulations no later than 90 days after termination of the service agreement.

8.3 The Processor may retain documentation that serves as proof of proper and contractual data processing, in accordance with the applicable retention periods, even beyond the end of the contract. Alternatively, the Processor may hand it over to the Controller at the end of the contract to discharge its responsibility. For the data retained in accordance with sentence 1, the obligations under paragraph 2 shall apply after the end of the retention period.

9. Sub-Processors

9.1 The Processor may engage additional processors (sub-processors). The basic requirements for the lawfulness of the processing shall remain unaffected. The Sub-Processors engaged to fulfil this contract are listed in detail in **Annex 2: List of Sub-Processors**. The Controller consents to their engagement. As this is a general written authorisation, the Processor shall inform the Controller promptly, but at least with a notice period of 4 weeks before the intended change with regard to the engagement or replacement of Sub-Processors. The Controller may object to such changes for a valid reason within this period. In the event of an objection, the Processor may terminate the contractual relationship with a notice period of 3 months. Services provided by third parties that support the execution of the contract, such as telecommunications services, are not considered subcontractor services under this provision. However, the Processor is obligated to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Controller's data, even when using outsourced ancillary services.

9.2 If subcontractors are engaged by the Processor, the Processor must ensure that its contractual agreements with the subcontractor are structured to ensure that the level of data protection is at least equivalent to the agreement between the Controller and the Processor, and that all contractual and legal requirements are met. This is particularly important regarding the implementation of appropriate Technical and Organisational Measures to ensure a satisfactory level of processing security.

9.3 The Controller is entitled, upon written request, to obtain information from the Processor about the content of the contract concluded with the subcontractor regarding the implementation of the subcontractor's data protection obligations.

9.4 If the subcontractor fails to meet its data protection obligations, the Processor shall be liable to the Controller for the subcontractor's compliance with these obligations. In such cases, the Processor must, at the Controller's request, terminate the subcontractor's engagement, either in whole or in part, or dissolve the contractual relationship with the subcontractor, provided this is not disproportionate.

10. Final Provisions

10.1 Changes and additions to this Annex and all its components require an agreement in the same form and an explicit indication that it constitutes a change or addition to these terms. This also applies to any waiver of this form requirement.

10.2 If this agreement requires written form, this requirement shall be satisfied by electronic formats.

10.3 The contract is governed by the law of the Federal Republic of Germany. The language of the proceedings is German. The place of jurisdiction is Koblenz.

10.4 Any right of retention by the Processor regarding personal data processed on behalf of the Controller and the associated data carriers, provided they are owned by the Controller, is excluded.

10.5 Should individual provisions of this agreement be invalid or unenforceable, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that most closely reflects the intent pursued by the Parties with the invalid or unenforceable provision. The above provisions shall apply accordingly in the event that the agreement proves to be incomplete.

Appendix 1: List of Persons Authorised to Issue Instructions.

1. **Authorised persons of the Controller**

Name: [Full name]
- Position: [Position in the company]
- Contact details: [E-mail address, telephone number]

Name: [Full name]
- Position: [Position in the company]
- Contact details: [E-mail address, telephone number]

(Additional persons can be listed here.)

2. **Authorised persons of the Processor (nuwacom GmbH)**

By name

Name: Sascha Böhr
- Position: CEO nuwacom GmbH
- Contact details: sascha.boehr@nuwacom.ai

Name: Alexander Kleinen
- Position: CTO nuwacom GmbH
- Contact details: alexander.kleinen@nuwacom.ai

By function
- The Account Manager of the Controller
- Employees of the Customer Success Department
- Employees of the Customer Support Department

Via their personal e-mail addresses or corresponding group e-mail addresses disclosed as part of customer support.

Changes to the persons authorised to issue instructions must be communicated in writing and by the persons authorised to issue instructions.

Appendix 2: List of Sub-Processors

Company, address	Scope of the contract	Scope of data processing, server location
Microsoft Ireland Operations, Ltd. **One Microsoft Place** **South County Business Park** **Leopardstown** Dublin 18, D18 P521, Ireland	Provision of the Azure Cloud infrastructure	Hosting Partner: Processes all personal data that the Processor processes for the Controller. Server location is EU.
Intercom R&D Unlimited Company 2nd Floor, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Irland	Customer support	Service provider for customer support software application. Server location is USA.
Amazon Web Services EMEA Sàrl, Avenue John F. Kennedy 38, 1855 Luxemburg *	LLM Hosting	Hosting Partner: Processes all personal data that the Processor processes for the Controller. Server location is EU.
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, Irland *	LLM Hosting	Hosting Partner: Processes all personal data that the Processor processes for the Controller. Server location is EU.
Mixpanel, Inc., One Front Street, Floor 28, San Francisco, CA 94111, USA	Product Analytics	Service provider for troubleshooting, optimization, and improvement. Server location is EU.

* Note: The controller has the option to hide or deactivate individual LLMs in the nuwacom software as needed.

Appendix 3: Technical and Organisational Measures.

1. **Physical Access Control**
   Measures to prevent unauthorised persons from gaining access to data processing systems that are used to process personal data:

   - The application is hosted in ISO 27001, ISO 27018 & SOC2-certified data centres. Access is severely restricted by a personalised access control system
   - The Processor's offices are secured and access is restricted to employees and authorised service providers (e.g. cleaning services) using personalised chip cards.
   - Guests are greeted at the door and accompanied to the contact person. The issue and return of access media is documented in writing.
   - Working from home: Unauthorised persons have no access to employees' homes.
   - Working from home: Instruct employees to work in work areas that are separate from living areas, if possible.

2. **System Access Control**
   Measures to prevent data processing systems from being used by unauthorised persons:

   - Access to data processing systems is restricted to authorised persons and requires identification and successful authentication by means of a user name and password using state-of-the-art security measures (e.g. MFA).
   - The data carriers on which the data processing systems are based use state-of-the-art encryption methods.
   - Access credentials are issued personally and are name-specific, no shared accounts are used.
   - Firewalls are used.
   - Use of housing interlocks.
   - Encryption of data carriers, smartphones and notebooks/tablets.

3. **Data Access Control**
   Measures to ensure that persons authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or deleted during processing without authorisation:

   - Access to the Controller’s data is restricted by a strict authorisation concept, which is implemented both organisationally and technically (Role Based Access Control Management). The assignment of authorisations is logged and reviewed at least once a year.
   - Access is logged and monitored. Logs are spot-checked for anomalies either manually on a random basis or automatically, where available.
   - Destruction of data carriers at least in accordance with DIN 66399.
   - The number of administrators is kept as small as possible.
   - Secure storage of data carriers.
   - User rights are managed by system administrators.

4. **Data Transfer Control**
   Measures to ensure that personal data cannot be read, copied, altered or deleted without authorisation during electronic transmission, transport or storage on data carriers, and that it is possible to verify and determine the entities to which personal data is intended to be transmitted using data transmission equipment:

   - The transmission of data is always encrypted (e.g. HTTPS using TLS 1.2, TLS 1.3). Mobile data carriers are encrypted.
   - Integrity checks ensure that data is transferred completely and is not corrupted.
   - Electronic encryption and signature procedures are implemented according to the state of the art (e.g. A+ rating, regular checks for weak ciphers)

5. **Input Control**
   Measures to ensure that it is possible to subsequently verify and determine whether and by whom personal data has been entered, modified or deleted in data processing systems:

   - Data processing systems use audit logs to ensure the traceability of changes to data records in a tamper-proof manner
   - Manual or automatic control of the logs
   - Creation of an overview of which applications can be used to enter, modify and delete which data
   - Traceability of data entry, modification and deletion by individual user names (not user groups)
   - Assignment of rights to enter, modify and delete data on the basis of an authorisation concept

6. **Processing Control**
   Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the Controller's instructions:

   - The Processor has defined appropriate processes and workflows for the processing of personal data. Implementation is regularly monitored by the internal data protection coordinator and the external data protection officer.
   - Employees receive annual training on security and data protection awareness. Participation is documented accordingly.
   - Persons who are authorised by the Processor to receive and carry out instructions are defined in the **Annex List of Persons Authorised to Issue Instructions**.
   - Written instructions to the Contractor or instructions in *"Textform" (a legal term specifically defined in § 126b of the BGB [German Civil Code], meaning a readable declaration on a durable medium, for example via email)*, (e.g. through a Data Processing Agreement)
   - Ensuring the destruction of data after completion of the contract, e.g., by requesting appropriate confirmations
   - Confirmation from Contractors that they obligate their own employees to confidentiality (typically in the Data Processing Agreement)
   - Careful selection of Contractors (especially with regard to data security)
   - Ensuring the destruction of data after completion of the contract, e.g., by requesting appropriate confirmations

7. **Availability Control**
   Measures to ensure that personal data is protected from accidental destruction or loss:

   - State-of-the-art and trusted service providers are used to support the provision of services. This includes in particular the use of redundant data centres and their own protection concepts.
   - Daily backups with a retention period of at least 30 and at most 90 days are available for recovery procedures. Generated backup versions are checked for integrity, and their suitability for recovery is ensured through regular backup & restore tests.
   - The application is scaled horizontally to ensure reliable failover processes.
   - Fire extinguishers in server rooms
   - Fire and smoke detection systems
   - Devices for monitoring temperature and humidity in server rooms
   - Air conditioning in server rooms
   - Protective socket strips in server rooms
   - Uninterruptible power supply (UPS)
   - RAID system / hard disk mirroring
   - Video surveillance in server rooms
   - Alarm notification in the event of unauthorised access to server rooms
   - Creation of a backup & recovery concept
   - Control of the backup process
   - Storage of data backups in a secure, off-site location
   - Creation of an emergency plan (e.g. BSI IT-Grundschutz 100-4)
   - Regular data recovery tests and logging of the results
   - No sanitary facilities in or above the server room
   - Separation of operating systems and data

8. **Separation Control**
   Measures to ensure that data collected for different purposes can be processed separately:

   - Test, staging and production systems are separated from each other.
   - The application provided to the Controller is designed as a separate tenant and is separated from other customers.
   - Within the application, the Controller has access to an authorisation management system, which logically separates data records from one another using row-level security.

9. **Procedures for regular review, assessment and evaluation**
   - Use of the heyData platform for data protection management
   - Appointment of the data protection officer heyData
   - Obligation of employees to maintain data confidentiality
   - Regular data protection training for employees
   - Maintaining an overview of processing activities (Art. 30 GDPR)
   - Carrying out annual data protection audits, including a review of Technical and Organisational Measures (TOMs)