Data Processing Agreement

Last updated: 27.10.2025

1. Preamble

This Data Processing Addendum ("DPA") forms part of the Service Agreement between Nuwacom (or "Processor") and Customer (or "Controller").

In providing the Services under the Agreement, Nuwacom may process Personal Data on behalf of the Customer in accordance with Applicable Data Protection Laws.

In the event of a conflict between this DPA and the Agreement, this DPA shall prevail.

2. Definitions

"Applicable Data Protection Law" refers to (i) the European General Data Protection Regulation 2016/679 (GDPR) and any applicable national data protection legislation, including in particular the Luxembourg *Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679*, (ii) the UK Data Protection Act 2018 ("UK GDPR"), or (iii) the Swiss Federal Act on Data Protection 1992 ("Swiss DPA").

"Authorized Sub-processors" means processors engaged by the Processor to assist in the fulfilment of its obligations. Sub-processors may also include third parties or Affiliates of the Processor.

"Personal Data Breach" means 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" means the 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.

"Sensitive Data" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under Applicable Data Protection Laws, which may include any of the following: biometric or health information; information 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.

"Service Agreement" means all relevant agreements and/or terms applicable to the Parties in connection with Nuwacom Services including, as applicable, the Nuwacom Terms of Service, the master services agreement, the Service Plan, and/or the Work Order, whichever are being applicable between the Parties.

"Supervisory Authority" means an independent authority responsible for monitoring the application of data protection law.

Controller, Data Subject, Processor, processing shall be interpreted within the meanings set out in the GDPR.

3. Scope of application

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 and Appendix 1.

3.3. Where enabled by the Customer, the Services may record, transcribe, and summarize meetings through the Nuwacom agent. Meeting recordings, transcripts, and summaries constitute Customer Data and are processed by Nuwacom solely on behalf of the Customer for the purpose of generating meeting summaries, follow-ups, and related analytics. The Customer determines which meetings are recorded and remains solely responsible for determining the lawful basis for such recording, obtaining any required notices or consents from participants, and configuring which meetings the Nuwacom agent may join. Where enabled by the Customer, the Services may record and temporarily or permanently store meeting audio and video for the purpose of enabling transcription, summarization, playback, and related note-taking functionalities. Nuwacom shall apply appropriate technical and organizational measures to protect the confidentiality and integrity of such recordings, including encryption in transit and at rest, access control, and secure deletion.

4. Responsibility and Authority to Issue Instructions

4.1. The Parties shall ensure compliance with Applicable Data Protection Laws. 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 forward requests to the Controller and provide reasonable and technically feasible help.

4.3. Where such assistance exceeds usual and reasonable effort, the Processor may charge the Controller for the costs incurred.

4.4. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Where required by Applicable Data Protection Laws, Customer shall configure and utilize the consent management features of the Services, including dual-party consent functionality, to ensure lawful recording, processing, and use of audio or other communications. Without limitation, Customer will provide all necessary notices to relevant Data Subjects, including a description of the Services, and secure all necessary permissions and consents, or other applicable lawful grounds for Processing Personal Data pursuant to this DPA and/or under Applicable Data Protection Laws, and shall indemnify, defend and hold harmless any claim, damages or fine against Nuwacom arising from any failure to acquire or use the Personal Data with legal consent or legitimate business purpose or in violation of any Applicable Data Protection Laws. Nuwacom will inform Customer, if in Nuwacom’s opinion an instruction infringes any provision under any Applicable Data Protection Laws and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the parties.

4.5. 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).

4.6. The Processor must immediately inform the Controller if the Processor believes that an instruction violates data protection regulations.

4.7. 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.

4.8. Except as otherwise authorized, the processing of Personal 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.

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 at http://trust.nuwacom.ai .

5. Compliance with Mandatory Legal Obligations by the Processor

5.1. The Processor shall ensure that the persons authorised to process Personal 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 Processor shall make available to the Controller the information necessary to demonstrate compliance 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). Such information may be provided through certifications, compliance reports, or other reasonable documentation that are available at http://trust.nuwacom.ai.

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.

6. Ensuring the Technical and Organisational Measures

6.1. The Parties agree that the Processor shall implement the technical and organisational measures described in the Trust Center at http://trust.nuwacom.ai and in Appendix 2.

6.2. These measures are deemed an integral part of this Agreement and may be updated by the Processor from time to time to reflect technical progress, provided that such updates do not reduce the overall level of security.

6.3. Technical and organisational measures are subject to technical progress. The Processor may implement alternative adequate measures, provided that such updates do not reduce the overall level of security of the Services.

6.4. Processor may use external auditors, from time to time, to verify the adequacy of its Personal Data processing security measures (each an "Audit"). Audits are performed at least once annually at Processor's expense by an independent auditor selected at Processor's discretion, such auditor delivering a confidential audit report (an "Audit Report"). Upon Controller's written request (and no more than once per annum), Processor will make available to Controller a copy of the most recent Audit Report. Controller agrees that the Audit Report satisfies any audit right granted by Applicable Data Protection Laws. If an Audit Report does not provide the sufficient necessary information or Controller is required to respond to a regulatory authority audit for which the Audit Report is not sufficient, then the Controller shall notify Processor at least ten (10) business days in advance, and the Parties shall develop a jointly agreed-upon audit plan that includes: (a) appointment an independent third party auditor; (b) the necessary access period during business hours; (c) billing to Controller at Processor's then-current rates; (d) occurs no more than once annually; and (f) restricts its findings to only data relevant to Controller. All information disclosed pursuant to this clause shall be treated as Confidential Information. 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. Personal Data Transfers

7.1. Processor shall only process Personal Data on documented instructions from Controller, including with regard to transfers of Personal Data to a third country or an

international organization, unless required to do so by Applicable Data Protection Laws to which Data Processor is subject. For purposes hereof, this DPA serves a set of documented Instructions from Controller to Processor.

7.2. The Controller authorizes Processor to transfer Personal Data to its Authorized Subprocessors including transfers to countries outside the Data Controller's country.

7.3. Before transferring Personal Data to a country different from where it was first collected, the Data Processor will take reasonable measures to comply with Applicable Data Protection Laws, including implementing appropriate safeguards where required.

7.4. Restricted Transfers outside the EEA and Switzerland: Where Customer is a Controller of the Personal Data protected by GDPR, then (i) Module 2 of the EU SCCs applies between Customer as "data exporter" and Nuwacom as "data importer" on the following basis: (ii) in Clause 7, the optional docking clause will apply, (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be fifteen (15) days; (iv) in Clause 11, the optional language shall not apply, (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Luxembourg law, (vi) in Clause 18(b), disputes shall be resolved before the courts of Luxembourg, (vii) For Annex 1, Parties' addresses, contact details, etc. are described in the definitions of the Parties provided in this DPA; the appointed contact person for the Processor is described in this DPA; the description of the transfer is set forth in Appendix 1 of this DPA, the competent supervisory authority shall be defined in accordance with clause 13 of the EU SCCs; (viii) Annex 2 to the EU SCCs will be deemed to incorporate Appendix 2 to this DPA and (xi) Annex 3 to the EU SCCs will be the Authorized Sub-processors. Where Customer is a Controller of Personal Data protected by the Swiss DPA, then Module 2 of the EU SCCs applies between Customer as "data exporter" and Nuwacom as "data importer" on the preceding basis and additionally: (i) in Clause 13 the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commission; (ii) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c), (iii) all references to GDPR in this Addendum are also deemed to refer to the Swiss DPA, and (iv) the EU SCCs also protect the Personal Data of legal entities until such time as a revised Swiss DPA enters into force.

7.5. Restricted Transfers outside the United Kingdom:

a. In respect of Personal Data subject to UK GDPR, the Parties agree (i) to rely on the Applicable EU SCCs as completed in Section 7.4 and as amended by the UK Addendum, (ii) the details shall be deemed to be completed as set forth in Section 7.4, (iii) the UK SCCs shall be incorporated by this reference and form an integral part of this DPA and that (iv) Data Controller shall be "Data Exporter" and Data Processor shall be "Data Importer".

b. The Applicable EU SCCS will have the following modifications (i) Table 1 of the UK Addendum shall be populated as follows: "Start date: As set forth in the Service Agreement, Parties' details: as set forth in this DPA and in the Service Agreement; and Key Contact: See this DPA and/or the Service Agreement"; (ii) Table 2 of the UK Addendum refers to the EU SCCs as defined in this DPA with details and applicable clauses described in Section 7.4; (iii) Table 3 of the UK Addendum shall be populated as follows: "The Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in: Annex 1A: List of Parties: as defined in the DPA, Annex 1B: Description of Transfer: as set forth in Appendix 1 and other sections of the DPA, Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as set forth in Appendix 2 of the DPA, Annex III: list of Sub processors: Authorized Sub-processors, and (iv) in Table 4 of the UK Addendum, either party may end the UK Addendum in accordance with its terms and the respective box for each is deemed checked.

c. Mandatory Clauses: the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of UK GDPR on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

8. Notification of Breaches by the Processor

The Processor shall inform the Controller without undue delay after becoming aware of a Personal Data Breach. 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 except where required by law..

9. Deletion and Return of Data

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

9.1. Upon 30 days following termination or expiration of the Service Agreement the Processor shall delete all Customer Data, 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 Applicable Data Protection Laws. A deletion log may be requested by the Controller in writing. Data sets may be returned to the Controller via the 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), if any, are deleted in accordance with Applicable Data Protection Laws no later than 90 days after termination of the Service Agreement.

9.2. 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 Service Agreement.

10. Sub-Processors

10.1. The Processor may engage additional processors (sub-processors). The basic requirements for the lawfulness of the processing shall remain unaffected. The current list of Authorized Sub-Processors is available at http://trust.nuwacom.ai. The Controller consents to their engagement. The Customer may object on reasonable grounds relating to data protection within fifteen (15) days of receiving such notice. If the Customer objects, the Parties will discuss in good faith to resolve the objection. 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.

10.2. If a new Sub-processor is engaged by the Processor, the Processor must ensure that its contractual agreements with the Sub-processor 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.

10.3. Information about the categories of Sub-processors engaged by the Processor and the nature of their data protection obligations is available at http://trust.nuwacom.ai. This information constitutes the Controller’s right of access under this Agreement. The Processor may provide additional information about sub-processor obligations upon written request where required to demonstrate compliance with applicable law.

10.4. If the Sub-processor fails to meet its data protection obligations, the Processor shall be liable to the Controller for the Sub-processor's compliance with these obligations.

11. Final Provisions

11.1. This Agreement may be updated by the Processor from time to time. Updates will be communicated to the Controller via the Trust Center or other suitable means. Continued use of the Services after 30 days constitutes acceptance of the updated Agreement.

11.2. Instructions from the Controller are limited to the configuration options available within the Services. Such instructions are deemed to be issued by the Controller through its authorised account administrators.

11.3. This agreement shall be governed by the laws of Luxembourg. The place of jurisdiction is Luxembourg City.

11.4. 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.

11.5. 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: Processing Operations

1. HOW WE COLLECT PERSONAL DATA

Nuwacom collects Personal Data through the following means: (i) Nuwacom Platform; (ii) Customer communications; (iii) AI Service providers and (iv) platform integrations.

2. DESCRIPTION AND NATURE OF PROCESSING ACTIVITIES AND SERVICES

General features: Services include the provision of an AI-driven data extraction and information processing tool, allowing users to upload or connect their own documents (contracts, reports, communications, etc.) and retrieve structured insights or answers.
Nuwacom agent: To provide automated meeting note-taking, transcription, and summarization functionality within the Nuwacom Platform, strictly on behalf of the Customer, and to store such summaries and transcripts in the Customer's workspace, and to enable the Customer to view, edit, or delete them.

3. 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.
- Nuwacom agent: Meeting participants

4. FREQUENCY OF PROCESSING
Continuous

5. CATEGORIES OF PERSONAL DATA PROCESSED AND SPECIFICS ON PROCESSING

- 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)

Nuwacom agent meeting recording and note-taking feature:

- Customer and Authorized Users determine the identity of the persons which are part of the conversations and content analyzed by the Services, and the type and nature of any Personal Data (if any) exchanged in such conversations or included in such content. Nuwacom has no control over the identity of the Data Subjects whose Personal Data is processed on behalf of Customer and over the types of Personal Data Processed. The Services are not intended for the Processing of Sensitive Data. At Customer's selection, the Services may also be used to capture voice identifiers relating to Authorized Users, for speaker identification and call cataloging purposes.
- Retention and Deletion. Unless otherwise instructed by the Customer, recordings and associated transcripts shall be retained only for as long as necessary to provide the Services or as configured by the Customer. When the Customer deletes a recording or terminates the relevant account, Nuwacom shall permanently and irreversibly delete the recording from active systems and remove it from backups within thirty (30) days.

Appendix 2: Technical and Organisational Measures.

Nuwacom's Technical and Organisational Measures can be found at http://trust.nuwacom.ai