

Translation Notice

This English version is provided as a translation for convenience. The German version under /legal/contracts/avv is the legally binding version.

Data Processing Agreement

Annex to the Terms and Conditions for the ConnectWunder software, which the controller confirms no later than during the first login to the ConnectWunder backend.

between

the user, legal entity, or natural person acting as an entrepreneur who receives the ConnectWunder services, hereinafter referred to as the "Client", "Controller", or "Controller".

hereinafter referred to as Client (Controller)

and

Yonju EOOD
ul.Brezovska 36 et.4
4003 Plovdiv
Bulgaria

hereinafter referred to as Processor

is agreed as an annex to the main contract identified above in accordance with the General Data Protection Regulation for the protection of the data of the Client processed by the Processor:

§ 1 Subject Matter and Term

(1) The subject matter of this contractual annex is the data processing carried out by the Processor for the Client within the scope of the main contract. This includes any processing of personal data within the scope of the main contract pursuant to Art. 28 GDPR.

(2) The purpose of the processing is the performance of the main contract by the Processor and the fulfillment of both parties' obligations under the GDPR.

(3) The term of this Agreement follows from its purpose. It runs for the duration of the main contract, including the fulfillment of warranty obligations or other post-contractual obligations by the Processor. If the main contract is terminated, this Agreement remains in force for the duration of the remaining post-contractual obligations and ends only upon full completion of the main contract and deletion or return of the data in accordance with this annex.

(4) Processing may take place in connection with the use of the ConnectWunder software, including booked or activated modules, interfaces, and functions. This may include in particular functions for organizing business relationships, communication, meetings, documents, work processes, artificial intelligence, automation, and interface connections. Details are set out in Annex 1.

§ 2 Type of Data, Data Subjects, Processing, Place of Contract

(1) This contractual annex applies to all types of processing pursuant to Art. 4 no. 2 GDPR.

(2) The type of data processed includes all data that the Processor processes for the Client within the scope of the main contract. The data is described in more detail in Annex 1 to

this Agreement.

(3) The categories of persons affected by this Agreement result from the Client's use of data and are described in more detail in Annex 1 to this contractual annex.

(4) Processing outside the European Union is possible only in cases permitted by law.

§ 3 Responsibility and Instructions

(1) This contractual annex does not change the fact that the Client remains solely responsible for compliance with data protection laws and lawful disclosure of the data to the Processor pursuant to Art. 4 para. 7 GDPR. This also applies to all processing that is the subject of this contractual annex.

(2) Instructions in the context of processing on behalf are first specified by the Client in the main contract. Subsequently, they may be issued orally or in text form. The Processor is entitled to require that oral instructions also be confirmed in text form without undue delay (for example email or other electronic form). Except in cases of imminent danger, the Processor may make execution of an instruction dependent on prior instruction in text form.

(3) Instructions that go beyond the content of the main contract are binding on the Processor only if they are required according to the purpose of the main contract and the provisions of the GDPR (for example safeguards required in an attack situation). They are at the same time an additional service under the main contract and must be remunerated additionally in accordance with the provisions there, or alternatively based on customary and reasonable remuneration.

(4) If the Processor is not obliged to execute an instruction, the Processor may refuse execution until the Client has confirmed and commissioned the additional service for a fee. Execution of the instruction does not constitute a waiver of any claim to additional remuneration.

(5) If execution of an instruction is unreasonable for the Processor, for example because compliance is technically impossible, the Processor may terminate the main contract unless the parties find another solution. An example is service provision by the Processor on a technical platform with other clients of processing on behalf where the instruction cannot be followed without consequences for other contractual partners of the Processor (for example data cannot be separated).

(6) If the Client issues an unlawful instruction, the Client bears the resulting costs, including the Processor's legal advice or representation costs.

(7) Instructions of the Client may also result from the use, administration, or configuration of the ConnectWunder software, in particular through settings within the platform, activated modules, connected interfaces, support requests, or documented electronic instructions of the Client.

(8) The Client remains responsible for the lawfulness of the Client's instructions. The Processor is not obliged to legally review the Client's instructions. However, if the Processor identifies an obvious violation of applicable data protection law or other law binding on the Processor, the Processor may suspend execution of the instruction until clarification.

§ 4 Obligations of the Processor

(1) The Processor is obliged to process the data only within the scope of the order and the Client's instructions. This does not apply where the Processor is obliged to carry out other processing under European Union law applicable to the Processor. The Processor may reject an instruction that violates applicable law that is also binding on the Processor and is not obliged to execute it. In such a case, the Processor will request that the Client issue a lawful instruction.

(2) The Processor supports the Client in fulfilling claims of data subjects under Arts. 12-23 GDPR within the Processor's capacities. The Processor names a data protection contact person to the Client.

(3) In the Processor's area, the Processor will comply with the obligations under Arts. 32 to 36 GDPR for the Client, taking into account the nature of the processing and the information available to the Processor, and will review them at appropriate intervals.

(4) The Processor organizes its operations to meet the special requirements of data protection. Pursuant to Art. 32 GDPR and taking into account the Processor's reasonable possibilities and facilities, the Processor implements technical and organizational measures that ensure the confidentiality, integrity, availability, and resilience of the systems and services related to processing on an ongoing basis. The current technical and organizational measures are set out in Annex 2 to this Agreement.

(5) The Processor ensures that employees and other third parties used in processing the Client's data are informed of data protection requirements and are appropriately instructed, trained, and supervised. The Processor further ensures that these persons are obliged not to process the data outside the Client's instructions and to treat the data confidentially, and that this confidentiality obligation continues after termination of the main contract.

(6) The Processor corrects, blocks, or deletes data that is the subject of this processing only in accordance with this Agreement or upon instruction of the Client. Such instructions of the Client are also binding after the contract.

(7) The Processor informs the Client if the Processor becomes aware that data of the Client has been or is being breached. The Processor independently takes the measures required to avert danger and secure the data and mitigates the consequences for the data subjects as far as possible. The Processor coordinates with the Client as quickly as possible.

(8) After completion of the processing activity, the Processor, at the Client's choice, either deletes all personal data or returns it to the Client. This does not apply to the extent the data must continue to be stored under applicable law or another provision results from the contract. If the Client issues no instruction, deletion is deemed agreed.

(9) To the extent the ConnectWunder software provides functions involving artificial intelligence, automated processing, transcription, summarization, communication analysis, media processing, interface connection, or automated data transfer, personal data is processed exclusively within the scope of the functions booked, activated, connected, or instructed by the Client. The Processor does not process personal data of the Client for the Processor's own purposes.

§ 5 Remuneration

(1) For all services under this Agreement, the Processor is entitled to additional remuneration in accordance with the main contract, or alternatively customary and reasonable remuneration. This does not apply to the extent the main contract expressly provides otherwise or such claims are excluded due to warranty or fault of the Processor.

(2) The remuneration obligation applies until full termination of this annex and does not end with the main contract.

§ 6 Obligations of the Client

(1) The Client may not issue any instruction that violates applicable law. The Client remains the controller for the data and is therefore responsible for informing itself about applicable laws, obtaining advice, and issuing only lawful instructions to the Processor.

(2) This applies in particular also to personal data that the Client introduces into or has processed through the ConnectWunder software in the context of communication functions, meeting or call processing, messaging, chat processing, transcription, media processing, artificial intelligence, automations, interfaces, writeback functions, or connected

third-party platforms. The Client is responsible for ensuring that the required legal bases, information obligations, and, where required, consents exist.

(3) The Client is in particular responsible for ensuring that meeting or call participants, communication partners, message recipients, chat partners, customers, prospects, employees, and other data subjects are properly informed to the extent required by applicable data protection laws or other statutory provisions.

(4) The Client is obliged to request and review the Processor's technical and organizational measures. The Client is responsible for ensuring that the Processor's measures constitute an appropriate level of protection for the risks of the data to be processed.

(5) The Client informs the Processor without undue delay and completely if facts become known to the Client indicating errors or irregularities in data processing.

(6) Upon request of the Processor, the Client names a contact person for all data protection questions at the Client's organization.

(7) The Client is obliged to process requests from data subjects for correction, deletion, blocking, or information. The Processor will refer the data subject to the Client if this is possible based on the data subject's information. The Processor is not liable if the data subject's request is not answered, not answered correctly, or not answered in due time by the Client.

§ 7 Evidence

(1) The Processor informs the Client about all measures for compliance with the requirements of Art. 28 GDPR and enables reviews within a reasonable scope. § 5 applies accordingly.

(2) The Processor is entitled to require a confidentiality declaration from the Client and/or the Client's auditor. The Client may appoint an independent external auditor if the Client provides the Processor with a copy of the audit report. Competitors of the Processor or persons otherwise unreasonable for the Processor may be rejected by the Processor.

(3) These rules apply accordingly to audits by an authority, including § 5.

(4) The Processor may primarily provide evidence through suitable documentation, security information, declarations, technical descriptions, or information about engaged subprocessors to the extent this enables appropriate evidence of compliance with the obligations under this Agreement. An on-site audit is required only where equivalent evidence cannot be provided in another reasonable way.

§ 8 Further Processors / Place of Processing

(1) Processing of the data on behalf takes place only in member states of the European Union (EU) or the European Economic Area (EEA). Processing of personal data in a third country is considered only if it is ensured that the legal requirements under Arts. 44-49 GDPR are met in order to ensure an adequate level of protection for personal data.

(2) The Processor is entitled to use further processors under Art. 28 GDPR in order to fulfill the contract.

(3) The further processors currently used are listed in Annex 3 to this Agreement. The Client consents to their use.

(4) The Processor will inform the Client if the Processor wishes to use other subcontractors. The Client may reject them if there is an important reason. If performance of the contract becomes unreasonable for the Processor due to rejection of a new subcontractor, the Processor may terminate the main contract within a reasonable period.

(5) The Client may be informed about new or replaced subprocessors also in text form, by email, through the platform, through a contact address named in the main contract, or by

updating an overview accessible to the Client. The Client may object within a reasonable period for good cause.

(6) The Processor is obliged to transfer the obligations under this Agreement to subcontractors.

(7) Subcontractors within the meaning of this provision are only companies that provide services directly in relation to the main service of the contract. Excluded from this are, in particular, ancillary services such as telecommunications, printing and transport services, as well as obligations relating to mere maintenance, disposal of data carriers, and measures to ensure the confidentiality, availability, integrity, and resilience of personal data, networks, services, data processing systems, and other IT systems. The Processor's obligation to ensure data protection and data security in relation to the Client's data remains unaffected.

§ 9 Liability and Damages

(1) If a data subject asserts claims for damages against a contractual party, the parties support each other and jointly contribute to clarification of the facts.

(2) Processor and Client are liable in accordance with Art. 82 GDPR for damages suffered by a data subject due to legally impermissible or incorrect data processing in this processing relationship.

§ 10 Final Provisions

(1) The main contract applies to dispute resolution, choice of law, and place of jurisdiction.

(2) This Agreement is concluded in text form and any amendment requires text form.

- Annex 1 - affected categories of data and persons
- Annex 2 - technical and organizational measures
- Annex 3 - subprocessors

Annex 1 - Affected Categories of Data and Persons

The Processor offers software that helps companies organize and structure business-related information, relationships, communication, meetings, documents, and operational processes in a central workspace and analyze and support them with artificial intelligence (AI).

The main functions of the software include, in particular, the management of persons and companies, meetings, notes, documents, communication histories, tasks, workflows, boards, interfaces, and automations. The software may also include modules for synchronous and asynchronous communication, in particular FlowListnr for meetings, calls, transcription and summaries, and FlowWritr for chat, messaging, and communication contexts, to the extent these are booked, activated, or used by the Client.

Type of Data	Nature and Purpose of Data Processing	Categories of Data Subjects

| Personal master data (for example salutation, last name, first name, address, title, profession) Communication data (for example email address, telephone number, chat or messenger identifier, communication history) Contract master data (for example contractual relationships, product and contract interests) Customer history and relationship data (for example leads, prospect status) Data that users independently transmit in messages, free-text fields, notes, documents, files, or other content | Purpose: Provision and operation of the ConnectWunder software Organization and structuring of business relationships, contacts, communication, meetings, documents, and operational processes Support for sales, customer care, account management, support, internal collaboration, and other business processes Provision of a central context layer for business-related information AI-supported analysis, structuring, summarization, and generation of content Nature: collection, organization, storage, arrangement, adaptation or alteration, retrieval, use, matching, restriction, deletion of data. | Users and employees of the Client Customers

of the Client Prospects and leads of the Client Business partners, contact persons, service providers, and other communication partners of the Client |

| Additionally when using FlowListnr: - Meeting and conversation data (for example meeting information, participant data, conversation content, notes, minutes, summaries) - Audio recordings or audio data, to the extent captured, activated, or introduced by the Client - Transcripts and derived summaries, tasks, insights, or meeting artifacts | Purpose: - Preparation, capture, transcription, structuring, and follow-up of meetings or calls - Creation of summaries, tasks, insights, or other meeting artifacts Nature: - collection, storage, transcription, organization, structuring, analysis, use, provision, transmission, restriction, and deletion of data | - Users and employees of the Client - Participants in meetings, calls, or other conversations - Customers, prospects, business partners, or other conversation partners of the Client |

| Additionally when using FlowWritr: - Chat, messaging, and communication content - Voice messages, images, media, attachments, or files, to the extent introduced or connected by the Client - Recipient and sender data - Communication metadata - Message drafts, suggestions, and, where applicable, writeback data | Purpose: - Processing, structuring, and provision of chat, messaging, and communication contexts - Creation of message drafts, suggestions, or communication histories - Transmission or writeback of communication content into connected systems or communication channels, to the extent activated or instructed by the Client Nature: - collection, storage, organization, structuring, analysis, use, provision, transmission, matching, restriction, and deletion of data | - Users and employees of the Client - Chat partners, recipients of messages, customers, prospects, business partners, or other communication partners of the Client |

| Technical data (IP address, log data, order ID) | Purpose: Technical support, maintenance, security, error analysis, and operation of the platform Nature: collection, recording, organization, storage, arrangement, adaptation or alteration, retrieval, use, matching, restriction, deletion of data. | Users and employees of the Client Other persons whose data is technically processed in the course of use |

Special Categories of Personal Data:

The ConnectWunder software is not designed to specifically process special categories of personal data pursuant to Art. 9 GDPR. Because the Client can itself introduce or connect content in the form of communication, meetings, chats, audio, media, documents, or free text into the platform, it cannot be excluded that such data is introduced into the platform by the Client or the Client's communication partners. The Client ensures that such data is processed only where legally permissible and appropriate safeguards have been implemented.

Annex 2 - Technical and Organizational Measures for Data Protection

Confidentiality (Art. 32 para. 1 lit. b GDPR):

- Access controls: personal and individual login, firewall
- Access authorization controls: encryption of data carriers
- Access to personal data by users of the Client according to the permissions assigned by the Client within the workspace
- Restricted visitor access to individual documents or boards, where technically provided
- Administrative access by the Processor only to the extent necessary for operation, support, security, or troubleshooting

Separation Controls:

- Separation of development and production environments
- Work computers: use of encrypted connections for access to cloud services
- Cloud services: logical separation of systems through different tenant capabilities of IT systems; use of cloud services that enable secure and separated processing of data
- Logical separation of workspaces and data of different clients within the platform

Integrity (Art. 32 para. 1 lit. b GDPR):

- Encryption of data carriers
- Secure file transfer or other data transport
- Protection against unauthorized alteration through access rights and permission concepts

Input Control

The following measures ensure that it can be checked who processed data in data processing systems and at what time:

- Access rights
- System-side logging
- Logging of security-relevant events and changes, where technically provided

Availability and Resilience (Art. 32 para. 1 lit. b GDPR):

- Regular backups
- For the availability and resilience of data stored or processed by Google Cloud, Firebase, OpenAI, or other subprocessors listed in Annex 3, we refer to the technical and organizational measures of these providers.

Processor Control:

- Data processing agreement
- Control of processing performance
- Selection of subprocessors taking into account suitable data protection guarantees
- Contractual obligation of subprocessors to data protection obligations

Additional Safeguards for Communication Data

To the extent the Client uses communication functions, meeting functions, call functions, messaging functions, transcription, media processing, or writeback functions, the following additional safeguards apply:

- Access to communication content occurs only to the extent required for provision, maintenance, security, error analysis, or support of the platform.
- Audio, transcript, message, media, and meeting data are processed only within the platform functionality and according to the Client's instructions.
- Administrative access to communication content is limited to required support, security, operational, or troubleshooting cases.
- Transcripts, messages, media, and meeting artifacts are processed within the platform using the intended authentication, authorization, and transport encryption mechanisms.
- Raw transcripts or comparable processing inputs may, where technically provided, be stored temporarily for processing. Permanent storage occurs only to the extent it is part of the respective platform functionality or configured accordingly by the Client.
- Content derived from raw transcripts, messages, or meeting data, in particular summaries, notes, tasks, decisions, documents, or other meeting artifacts, may be stored as regular platform data.
- Sending, synchronization, or writeback into connected systems or communication channels occurs only to the extent the Client has deliberately set up the respective integration, trigger, agent, or other automation, or has manually triggered a specific action, and only within the technically intended scope of service.

In addition, the Client remains responsible for the lawful setup, configuration, and use of communication, transcription, media processing, integration, and writeback functions, in particular for required information obligations, consents, and permissions vis-a-vis data subjects, as well as for required access rights, approvals, and configurations in connection with connected third-party platforms.

Reference to Technical and Organizational Measures of Subprocessors:

- The availability, integrity, and security of the data stored or processed by Google Cloud, Firebase, OpenAI, or other subprocessors listed in Annex 3 are subject to the technical and organizational measures of these providers. Further details about these measures are available in the respective security documentation, privacy policies, or data processing agreements of the providers.

Reference Documentation of Subprocessors:

1. Google Cloud & Firebase:

1. Security documentation: <https://cloud.google.com/trust-center/security?hl=en>
(<https://cloud.google.com/trust-center/security?hl=en>)
2. Privacy Policy: Google Cloud Privacy (<https://cloud.google.com/privacy>)

3. Cloud Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum>
(<https://cloud.google.com/terms/data-processing-addendum>)
4. Data center encryption measures and certificates:
<https://cloud.google.com/docs/security/encryption/default-encryption>
(<https://cloud.google.com/docs/security/encryption/default-encryption>)
<https://cloud.google.com/security/compliance/iso-27001/>
(<https://cloud.google.com/security/compliance/iso-27001/>)
2. OpenAI:
 1. Security documentation: OpenAI Security (<https://openai.com/security>)
 2. Privacy Policy: OpenAI Privacy (<https://openai.com/privacy>)
3. ElevenLabs:
 1. Security documentation / Trust Center: <https://compliance.elevenlabs.io/>
(<https://compliance.elevenlabs.io/>)
 2. Privacy Policy: <https://elevenlabs.io/privacy-policy>
(<https://elevenlabs.io/privacy-policy>)
 3. Data Processing Addendum: <https://elevenlabs.io/dpa> (<https://elevenlabs.io/dpa>)

Annex 3 - Subprocessors in the Context of Processing on Behalf

Name and Address of Subprocessor Description of Partial Services	
----- -----	
Google Firebase 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Storage of user data and interaction data in the Europe cloud region
Google Cloud 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Product provision through product hosting in the Europe cloud region
OpenAI 3180 18th Street, San Francisco, CA 94110, USA	AI-supported processing, analysis, structuring, summarization, and generation of content, as well as answering user requests, to the extent OpenAI is used for the respective function
ElevenLabs Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA	AI-supported audio processing, in particular transcription, analysis, and processing of audio content, to the extent ElevenLabs is used for the respective function

To the extent subprocessors outside the European Union or the European Economic Area are used, or access from a third country occurs, this takes place only in compliance with the statutory requirements of Arts. 44 to 49 GDPR, in particular through suitable safeguards such as standard contractual clauses or other legally provided protection mechanisms.