DATAPROCESSING AGREEMENT (DPA)

pursuant to Art. 28 GDPR

between

customers who use a software-as-a-service product of awork GmbH

– hereinafter referred to as the "Customer" –

and

the processor

awork GmbH

Großer Burstah 36/38 · 20457 Hamburg, Germany

– hereinafter referred to as the "Processor" –

PREAMBLE

The terms and definitions of Regulation (EU) 2016/679 (hereinafter "GDPR"), in particular of Art. 4 GDPR, apply to this Data Processing Agreement.

1. SUBJECT MATTER

1.1 The subject matter of this Data Processing Agreement is the determination of the data protection framework for the contractual relationship between the parties.

1.2 The description of the respective processing, including the subject matter of the processing, its scope, nature and purpose, the type of personal data and the categories of data subjects, is set out in Annexes 1A and 1B.

2. LOCATION OF DATA PROCESSING

2.1 The contractually agreed processing takes place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state to the Agreement on the European Economic Area ("Safe Countries"), unless the Annex provides otherwise.

2.2 The Processor may process Customer data, or have it processed, by entities outside the Safe Countries ("Third Country") only if and to the extent that (i) an adequate level of data protection has been established for the relevant Third Country on the basis of a valid decision of the European Commission, or (ii) the processing is carried out on the basis of and in accordance with the applicable EU Standard Contractual Clauses ("SCC"), which are to be presented to the Customer and agreed in writing with the entity established in the Third Country ("Data Importer"). If the Data Importer and the Processor are not identical, the Processor shall accede to these SCC. The provisions set out in this DPA remain unaffected.

3. TERM

3.1 This agreement is concluded for an indefinite period and may be terminated by either party with three months' notice. If, at the time of termination, one or more main agreements under which the Processor processes personal data of the Customer on its behalf are still in force, the provisions of this agreement shall continue to apply until the regular termination of the main agreement(s).

3.2 The Customer may terminate this agreement without notice if the Processor commits a serious breach of data protection regulations or of the provisions of this agreement. In particular, non-compliance with the obligations agreed in this agreement and derived from Art. 28 GDPR constitutes a serious breach.

4. INSTRUCTIONS

4.1 The Processor processes the personal data only within the scope of the instructions issued by the Customer. This does not apply to the extent that the Processor is obliged to process the data under EU law or the law of the member states to which the Processor is subject. In this case, the Processor shall

notify the Customer of these legal requirements before the processing, unless the relevant law prohibits such notification on important grounds of public interest.

4.2 If instructions change, revoke or supplement the provisions made in the applicable Annexes 1A and 1B of this agreement, they are permissible only if a corresponding new agreement is made in written form.

4.3 Irrespective of the form in which they are issued, both the Processor and the Customer shall document every instruction of the Customer in text form. The instructions are to be retained for the duration of this agreement and for a further three years thereafter.

4.4 The Processor shall inform the Customer without undue delay if, in its opinion, an instruction issued by the Customer violates statutory provisions. In such a case, the Processor is entitled, after giving the Customer timely prior notice, to suspend the execution of the instruction until the Customer has amended or confirmed it. If the Processor can demonstrate that processing in accordance with the Customer's instruction may result in liability of the Processor under Art. 82 GDPR, the Processor is free to suspend further processing in that respect until the question of liability has been clarified between the parties.

4.5 Instructions may only be issued by persons who represent the Customer in this respect by virtue of their corporate position or their particular function (e.g. data protection officer, chief security officer, etc.).

4.6 The Processor designates the recipients of instructions in the Annex to this agreement. In the event of a change or a prolonged absence of the contact persons, the successors or deputies shall be notified to the contracting party without undue delay in written or electronic form.

5. SUPPORT OBLIGATIONS OF THE PROCESSOR

5.1 Taking into account the nature of the processing, the Processor shall take appropriate technical and organisational measures to assist the Customer in fulfilling its obligation to respond to requests from data subjects under Arts. 12 to 22 GDPR.

5.2 Taking into account the nature of the processing and the information available to it, the Processor shall assist the controller in complying with its obligations under Arts. 32 to 36 GDPR. This applies in particular to the security of processing, the notification of personal data breaches to the supervisory authority, the communication of a personal data breach to data subjects, the data protection impact assessment and the prior consultation of the competent supervisory authority.

5.3 If a data subject or a data protection supervisory authority contacts the Processor directly in connection with the personal data processed under this agreement, the Processor shall inform the Customer without undue delay and coordinate further steps with the Customer.

6. AUDIT RIGHTS OF THE CUSTOMER

6.1 Upon the Customer's request, the Processor shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this agreement and in Art. 28

GDPR. In particular, the Processor shall provide the Customer with information about the stored data and the data processing programs.

6.2 The Customer or third parties commissioned by the Customer are entitled – in principle after prior notice of at least 30 days – to verify compliance with the obligations under this agreement and Art. 28 GDPR and to carry out on-site inspections at the Processor. The Processor shall enable and contribute to this. Inspections without a specific reason are limited to a maximum of one inspection per year.

6.3 Upon request, the Processor shall provide the Customer with suitable evidence of compliance with the obligations pursuant to Art. 28(1) and (4) GDPR. This evidence may be provided by submitting documents and certificates demonstrating approved codes of conduct within the meaning of Art. 40 GDPR or approved certification procedures within the meaning of Art. 42 GDPR.

7. DATA PROTECTION OFFICER OF THE PROCESSOR

7.1 The Processor's data protection officer is stated in Section 3 of the Annex to this agreement.

8. CONFIDENTIALITY

8.1 The Processor confirms that it is familiar with the data protection provisions of the GDPR relevant to the processing. When processing the Customer's personal data, it shall maintain data secrecy and confidentiality. This obligation continues after the termination of this contractual relationship.

8.2 The Processor warrants that it will familiarise the employees engaged in performing the work with the data protection provisions applicable to them. It shall bind these employees by written agreement to maintain confidentiality during their activity and after the termination of their employment, unless they are subject to an appropriate statutory duty of confidentiality. The Processor monitors compliance with data protection regulations in its company.

8.3 The Processor may provide information to third parties or data subjects only with the prior written consent of the Customer, or consent in an electronic format.

9. TECHNICAL AND ORGANISATIONAL MEASURES

9.1 The Processor shall implement appropriate technical and organisational measures so that the processing complies with the requirements of the GDPR and the protection of the rights of the data subject is ensured. It shall design its internal organisation so that it meets the specific requirements of data protection and achieves an appropriate level of protection. In particular, taking into account the respective state of the art, the Processor shall ensure appropriate security of processing, in particular the confidentiality (including pseudonymisation and encryption), availability, integrity and resilience of the systems and services used for data processing.

9.2 The technical and organisational measures set out in the Annex are agreed as binding.

9.3 In the course of the contractual relationship, the technical and organisational measures may be adapted to technical progress. The adapted measures must at least correspond to the level of security of the measures agreed in the Annex. Material changes are to be agreed in written form or in an electronic format.

10. INFORMATION OBLIGATIONS OF THE PROCESSOR AND PERSONAL DATA BREACHES

10.1 The Processor shall inform the Customer without undue delay of any breaches or suspected breaches of this agreement or of provisions concerning the protection of personal data.

10.2 The Processor shall support the Customer in investigating, mitigating and remedying the breaches.

10.3 If the personal data processed under this agreement are put at risk at the Processor by attachment or seizure, by insolvency or composition proceedings, or by other events or measures of third parties, the Processor shall inform the Customer without undue delay. The Processor shall also inform all relevant bodies in this context without undue delay that control over the data lies with the Customer.

10.4 Where inspections by data protection supervisory authorities are carried out, the Processor undertakes to disclose the result to the Customer, insofar as it concerns the processing of personal data under this agreement. The Processor shall remedy the deficiencies identified in the inspection report without undue delay and inform the Customer accordingly.

11. SUB-PROCESSORS

11.1 The Customer authorises the Processor to engage sub-processors in the processing. No separate prior consent of the Customer is required. The Processor shall inform the Customer in text form of any intended change concerning the engagement or replacement of a sub-processor at least 6 weeks before the planned changeover. The Customer may object to the change in text form for good cause within 3 weeks of receipt of the information. An objection entitles both parties to extraordinary termination of the main agreement. If no objection is raised within the period, consent is deemed to have been given.

11.2 The Processor shall contractually ensure that the provisions agreed in this agreement also apply to sub-processors. The Processor's contract with the sub-processor must be concluded in writing or in electronic format.

11.3 Sub-processors in third countries shall be engaged only if the special requirements of Art. 44 et seq. GDPR are met.

11.4 The Customer hereby also expressly consents to the engagement of the sub-processors listed in the applicable Annexes.

11.5 The Processor shall ensure that the Customer has the same rights of instruction and control vis-à-vis the sub-processor as vis-à-vis the Processor under this agreement. If a sub-processor fails to comply with its data protection obligations, the Processor shall be liable to the Customer for the compliance of that sub-processor with its obligations.

11.6 Upon the Customer's request, the Processor shall demonstrate to the Customer the conclusion of the agreements entered into with the sub-processor. The evidence shall be provided in text form.

12. DELETION AND RETURN OF PERSONAL DATA

12.1 Upon completion of the processing services agreed in the respective main agreement, the Processor is obliged to delete all personal data it has received in the course of the processing within 35 days. This

includes in particular the results of the data processing, documents and data carriers provided, and copies of the personal data. The obligation to delete does not apply if the Processor is legally obliged under EU law or the law of the member states to continue storing the data. If there is a further obligation to store, the Processor shall restrict the processing of the personal data and use the data only for the purposes for which the obligation to store exists. The obligations regarding the security of processing continue for the period of storage. The Processor shall delete the data within 35 days once the obligation to store ceases.

Where multiple services are used within a shared workspace, personal data required to continue providing a remaining subscribed service shall be exempt from deletion solely due to the termination of another service. Such data shall continue to be processed in accordance with the applicable Data Processing Agreement and the customer's instructions.

12.2 Deletion shall be carried out in such a way that the data cannot be restored.

12.3 The processes shall be logged, stating the date.

12.4 At the Customer's request, personal data that the Processor has received from the Customer in the course of the processing shall be returned to the Customer within 35 days after completion of the processing services agreed in the respective main agreement.

13. LIABILITY

13.1 The parties are liable in accordance with Art. 82 GDPR.

13.2 In the internal relationship, the Processor is liable to the Customer only for fault lying within its sphere. The liability provisions of the main agreement remain unaffected in the internal relationship.

14. FINAL PROVISIONS

14.1 The defence of a right of retention within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the data processed for the Customer.

14.2 The Annex or, in the case of several main agreements concluded, the Annexes to this agreement form an essential part of it.

14.3 Amendments or collateral agreements require written form or an electronic format. This also applies to amendments to this formal requirement.

14.4 Insofar as agreements on data processing on behalf of a controller already exist between the parties with regard to the services specified or referred to in this DPA, these agreements are superseded as of the effective date of this DPA, and this DPA conclusively governs the rights and obligations of the parties in this respect.

14.5 The parties agree that this DPA is to be signed by means of an electronic signature and may alternatively be executed in written form. It may be validly signed by electronic signature in such a way that the parties exchange the copies signed by them in electronic form as PDF files. Signing may also be effected through the Processor's digital online registration process. The Customer warrants that the person signing or completing the online registration process (authorised representative) holds

all powers of attorney and powers of representation required to conclude this DPA. The Customer shall be bound by all declarations of the authorised representative. Amendments to this DPA, including its Annexes, are likewise subject to the formal requirements set out in this Section.

14.6 If any provision of this agreement proves to be invalid, the validity of the remaining provisions of the agreement shall not be affected.

14.7 This DPA is governed by German law. The place of jurisdiction for disputes arising from this DPA corresponds to the provision of the main agreement.

ANNEXES TO THE DATA PROCESSING AGREEMENT

Annex 1A applies to awork, including the optional AI functions contained therein. Annex 1B applies to awork AI. If both services are booked, both Annexes apply.

ANNEX 1A – DESCRIPTION OF THE PROCESSING FOR awork

1A.1 SUBJECT MATTER OF THE PROCESSING

The Processor is a manufacturer and provider of enterprise software for handling all project-related commercial processes. This includes the sale, consulting, implementation and integration, hosting and support of the solutions. The collection, processing and use of data takes place for the purposes stated above.

1A.2 SCOPE, NATURE (ART. 4(2) GDPR) AND PURPOSE OF THE DATA PROCESSING

Personal data is processed for the purpose of providing the software-as-a-service application awork, which the Customer uses to organise its work, teams and projects. This means in particular:

- Hosting (data, application, system, components)
- Operation (application, system, components)
- Maintenance (application, system, components)
- Support (application, system, components)
- Further development (application, system, components)

For this purpose, personal data is collected, stored, retrieved, organised and arranged, displayed in user interfaces and deleted.

1A.2.1 SUPPLEMENTARY OPTIONAL AI PROCESSING

Where AI-supported functions are available in the booked awork plan, the following processing takes place only if the relevant function or model has been enabled for the workspace and is actually used or configured by the Customer or its users:

- Transmission and temporary processing of prompts, selected workspace content and the context required for the request in order to generate text, image or other model outputs
- Storage of chat histories and AI content saved by the user exclusively in the Azure infrastructure controlled by awork, so that they can be displayed in the product

- Execution of agents, tools, connections, triggers and schedules within the permissions granted by the Customer
- No use of Customer data to train general models and no storage of prompts or outputs by the model inference providers used
- No use of AWS Bedrock as a failover or peak-load fallback for the regular Azure-based AI processing

Authorised workspace administrators can deactivate available models in accordance with the product functionality. Deactivated models are not used for new processing.

1A.3 CATEGORIES OF DATA SUBJECTS AND TYPES OF DATA

Personal data is collected, processed and used for the following groups of persons, insofar as this is necessary to fulfil the stated purpose:

- Internal and external employees (e.g. freelancers) and temporary staff of the Customer
  - Professional contact and (work) organisational data for user administration: surname, first name, gender, email, telephone number, photo
  - Data on professional circumstances: job title, log file information, IP address, working time, absence times, activities
- Prospects, customers and other business partners of the Customer
  - Professional contact and (work) organisational data: surname, first name, email, telephone number
- When optional AI functions are used, additionally
  - Content from prompts, selected workspace context, documents and files, and model outputs
  - Agent configurations, tool calls and agent/tool activity information
  - Other personal data that the Customer releases for processing; special categories under Art. 9 GDPR only insofar as the Customer enters or releases such data on its own responsibility

1A.4 LIST OF SUB-PROCESSORS

The awork application can be used without AI data processing; AI functions of awork can be deactivated by the administrator. Providers designated as optional or conditional are used only if the designated function or model is enabled for the workspace.

A. GENERAL PLATFORM SERVICES

Microsoft Ireland Operations Limited – Azure Compute/Storage

Subject matter of service	Primary hosting. Provision of the technical infrastructure for the operation of awork in German data centres; includes servers, storage and network services.
Data processed	All data listed under Annex 1A.2; all data entered into awork, e.g. projects, tasks, time entries and documents; user and access permissions; uploaded files and content.
Location	Germany: Frankfurt am Main (Germany West Central) and Berlin (Germany North). All customer data is stored and processed exclusively in Germany.
Safeguards	DPA with Microsoft; ISO 27001, SOC 2 and BSI C5; encryption of all data in transit and at rest; strict access controls based on the principle of least privilege; no transfer of customer data outside Germany.

Microsoft Ireland Operations Limited – Azure Front Door/CDN

Subject matter of service	Fast and secure delivery of the awork application via a global content delivery network, and protection against cyberattacks.
Data processed	Technical connection data, in particular IP address and browser information; cached static app resources such as images, scripts and stylesheets; no processing of business data.
Location	Primarily EU/Germany: customer data is stored and processed in the selected EU region. Only when accessed from a non-EU country may technically necessary, short-term processing of technical connection data take place via the geographically nearest server; stored content is not affected.
Safeguards	DPA with Microsoft; EU data residency for customer data; encrypted transmission; technical connection data is stored for a maximum of 30 days; no permanent storage of business content in the CDN; in the case of technically necessary third-country processing, an adequacy decision or SCC apply.

Birdie.so / Philo Labs

Subject matter of service	Tool for error capture and reporting. Becomes active only when a user themselves reports a bug using a screen recording; captures technical context information for faster problem resolution.
Data processed	Error description and comments; automatically captured technical data such as browser, operating system and console logs; screenshots or screen recordings optionally added by the user; basic user data such as name and email for feedback.
Location	EU: Paris, France.
Safeguards	DPA with guaranteed exclusive EU processing; no third-country transfer; encrypted data transmission; data minimisation to bug-relevant information; automatic deletion after 90 days following ticket processing. Business data is not transferred automatically.

Twilio Ireland Limited – Segment

Subject matter of service	Exclusively forwarding of technical data and context to Intercom for the provision and improvement of customer support
Data processed	technical usage and device data, account/user context for support purposes and, where applicable, support-related content submitted by the user
Location	primarily EU: processing in the USA within the Twilio infrastructure possible
Safeguards	DPA; EU-US Data Privacy Framework; SCC as additional safeguard; data minimisation

Intercom, Inc.

Subject matter of service	Customer support and support communication in awork
Data processed	<u>In case of support contact:</u> a) Name, email, chat history b) Content shared by the user (e.g. screenshots) <u>In case of system messages:</u> a) Email address for important updates
Location	USA
Safeguards	DPA; EU-US Data Privacy Framework; SCC as additional safeguard; ISO 27001/SOC 2; encrypted transmission; data minimisation

B. OPTIONAL AI INFRASTRUCTURE AND MODEL INFERENCE

Microsoft Ireland Operations Limited – Azure AI Foundry · optional/conditional

Subject matter of service	AI functions in awork (project management software)
Data processed	Prompts, required workspace context and generated text or image outputs
Location of processing	EU: Primarily Germany West Central, fallback resource Sweden Central
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories are stored exclusively in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Microsoft - Encrypted transmission of data - Integrated security and content filters - AI functions can be deactivated per workspace by administrators - No direct access by OpenAI to prompts or model outputs

Google Cloud – Vertex AI API · optional/conditional

Subject matter of service	Provision of selected Google/Gemini text and image models
Data processed	Prompts, required workspace context and generated outputs
Location of processing	EU: Google Cloud region Europe-West1, Belgium
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories remain in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Google - Encrypted transmission of data - Processing in the designated Google Cloud region in Belgium - Integrated and configurable safety filters check inputs and outputs for harmful content and can block it - Use of the models provided via Google can be deactivated per workspace by administrators

Amazon Web Services EMEA SARL – Amazon Bedrock Runtime · optional/conditional

Subject matter of service	Provision of selected Anthropic models
Data processed	Prompts, required workspace context and generated outputs
Location of processing	European Union: Germany (eu-central-1), Ireland (eu-west-1), France (eu-west-3), Sweden (eu-north-1), Italy (eu-south-1) and Spain (eu-south-2). Inference requests may be processed within these AWS regions; no global processing takes place.
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories remain in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Amazon Web Services - Encrypted transmission of data - Exclusive use of geographically restricted EU inference profiles - No access by the model providers to prompts or model outputs - Use of the models provided via AWS can be deactivated per workspace by administrators - Security and content filters via Amazon Bedrock Guardrails

TensorX Limited · optional/conditional

Subject matter of service	Provision of selected open-source AI models, currently Qwen, GLM, Kimi and DeepSeek
Data processed	Prompts, required workspace context and generated outputs
Location of processing	Exclusively within the EEA on TensorX-owned hardware in Dublin, Ireland, and Helsinki, Finland
Storage and training	No storage or logging of prompts and model outputs; no use for training purposes; processing of inference data exclusively in volatile memory on TensorX-owned hardware; no disclosure to model providers
Safeguards and controls	- Data processing agreement with TensorX - Processing exclusively in volatile memory on own hardware - No disclosure of inference data to the model providers

OpenAI Ireland Ltd. – OpenAI API / AI model inference · optional/conditional

Subject matter of service	Provision of selected AI models for AI functions in awork.
Data processed	Prompts, required selected content and workspace context, and generated outputs, insofar as the respective function uses OpenAI.
Location of processing	Processing of customer content via the European processing region agreed and configured for the deployment. The geographic requirements and, where applicable, safeguards for third-country processing are governed by the applicable data processing agreement with OpenAI and the activated processing settings.
Storage and training	No use of customer content transmitted for model inference to train general models. For the API processing used, zero data retention and the required regional processing settings have been agreed and activated; technically necessary or contractually permitted exceptions remain unaffected in accordance with the applicable provider terms.
Safeguards	Data processing agreement with OpenAI, encryption in transit, technical access controls, and agreed regional processing and retention settings.

ANNEX 1B – DESCRIPTION OF THE PROCESSING FOR awork AI

1B.1 SUBJECT MATTER OF THE PROCESSING

The Processor is a manufacturer and provider of enterprise software for the AI-supported processing of information and the support of workflows. This includes the sale, consulting, implementation and integration, hosting and support of the solutions. The collection, processing and use of data takes place for the purposes stated above.

1B.2 SCOPE, NATURE (ART. 4(2) GDPR) AND PURPOSE OF THE DATA PROCESSING

Personal data is processed for the purpose of providing the software-as-a-service application awork AI, which the Customer uses for the AI-supported processing of information and the support of its workflows. This means in particular:

- Hosting (data, application, system, components)
- Operation (application, system, components)
- Maintenance (application, system, components)
- Support (application, system, components)
- Further development (application, system, components)

For this purpose, personal data is collected, stored, retrieved, organised and arranged, displayed in user interfaces and deleted.

1B.2.1 AI PROCESSING

In the course of providing and using awork AI, the AI processing described below takes place in particular.

- Transmission and temporary processing of prompts, selected workspace content and the context required for the request in order to generate text, image or other model outputs
- Storage of chat histories and AI content saved by the user exclusively in the Azure infrastructure controlled by awork, so that they can be displayed in the product
- Execution of agents, tools, connections, triggers and schedules within the permissions granted by the Customer
- No use of Customer data to train general models and no storage of prompts or outputs by the model inference providers used

1B.3 CATEGORIES OF DATA SUBJECTS AND TYPES OF DATA

Personal data is collected, processed and used for the following groups of persons, insofar as this is necessary to fulfil the stated purpose:

- Internal and external employees (e.g. freelancers) and temporary staff of the Customer
  - Professional contact and (work) organisational data for user administration: surname, first name, gender, email, telephone number, photo
  - Data on professional circumstances: job title, log file information, IP address, working time, absence times, activities

- Prospects, customers and other business partners of the Customer
  - Professional contact and (work) organisational data: surname, first name, email, telephone number

In addition, the following data may contain personal data in the course of AI processing:

- Content from prompts, selected workspace context, documents and files, and model outputs
- Agent configurations, tool calls and agent/tool activity information
- Other personal data that the Customer releases for processing; special categories under Art. 9 GDPR only insofar as the Customer enters or releases such data on its own responsibility

1B.4 LIST OF SUB-PROCESSORS

Providers designated as optional or conditional are used only if the designated function or model is available and enabled for the workspace.

A. GENERAL PLATFORM SERVICES

Microsoft Ireland Operations Limited – Azure Compute/Storage

Subject matter of service	Primary hosting. Provision of the technical infrastructure for the operation of awork AI in German data centres; includes servers, storage and network services.
Data processed	All data listed under Annex 1B.2; all data entered into awork AI, e.g. projects, tasks, time entries and documents; user and access permissions; uploaded files and content.
Location	Germany: Frankfurt am Main (Germany West Central) and Berlin (Germany North). All customer data is stored and processed exclusively in Germany.
Safeguards	DPA with Microsoft; ISO 27001, SOC 2 and BSI C5; encryption of all data in transit and at rest; strict access controls based on the principle of least privilege; no transfer of customer data outside Germany.

Microsoft Ireland Operations Limited – Azure Front Door/CDN

Subject matter of service	Fast and secure delivery of the awork AI application via a global content delivery network, and protection against cyberattacks.
Data processed	Technical connection data, in particular IP address and browser information; cached static app resources such as images, scripts and stylesheets; no processing of business data.
Location	Primarily EU/Germany: customer data is stored and processed in the selected EU region. Only when accessed from a non-EU country may technically necessary, short-term processing of technical connection data take place via the geographically nearest server; stored content is not affected.
Safeguards	DPA with Microsoft; EU data residency for customer data; encrypted transmission; technical connection data is stored for a maximum of 30 days; no permanent storage of business content in the CDN; in the case of technically necessary third-country processing, an adequacy decision or SCC apply.

Birdie.so / Philo Labs

Subject matter of service	Tool for error capture and reporting. Becomes active only when a user themselves reports a bug using a screen recording; captures technical context information for faster problem resolution.
Data processed	Error description and comments; automatically captured technical data such as browser, operating system and console logs; screenshots or screen recordings optionally added by the user; basic user data such as name and email for feedback.
Location	EU: Paris, France.
Safeguards	DPA with guaranteed exclusive EU processing; no third-country transfer; encrypted data transmission; data minimisation to bug-relevant information; automatic deletion after 90 days following ticket processing. Business data is not transferred automatically.

Twilio Ireland Limited – Segment

Subject matter of service	Exclusively forwarding of technical data and context to Intercom for the provision and improvement of customer support
Data processed	technical usage and device data, account/user context for support purposes and, where applicable, support-related content submitted by the user
Location	primarily EU: processing in the USA within the Twilio infrastructure possible
Safeguards	DPA; EU-US Data Privacy Framework; SCC as additional safeguard; data minimisation

Intercom, Inc.

Subject matter of service	Customer support and support communication in awork AI
Data processed	In case of support contact: a) Name, email, chat history b) Content shared by the user (e.g. screenshots) In case of system messages: a) Email address for important updates
Location	USA
Safeguards	DPA; EU-US Data Privacy Framework; SCC as additional safeguard; ISO 27001/SOC 2; encrypted transmission; data minimisation

B. OPTIONAL AI INFRASTRUCTURE AND MODEL INFERENCE

Microsoft Ireland Operations Limited – Azure AI Foundry

Subject matter of service	AI functions in awork AI. In addition, provision of low-cost AI models that are used automatically as soon as the Customer's AI credits are used up.
Data processed	Prompts, required workspace context and generated text or image outputs
Location of processing	EU: Primarily Germany West Central, fallback resource Sweden Central
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories are stored exclusively in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Microsoft - Encrypted transmission of data - Integrated security and content filters - No direct access by OpenAI to prompts or model outputs

Google Cloud – Vertex AI API · optional/conditional

Subject matter of service	Provision of selected Google/Gemini text and image models
Data processed	Prompts, required workspace context and generated outputs
Location of processing	EU: Google Cloud region Europe-West1, Belgium
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories remain in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Google - Encrypted transmission of data - Processing in the designated Google Cloud region in Belgium - Integrated and configurable safety filters check inputs and outputs for harmful content and can block it - Use of the models provided via Google can be deactivated per workspace by administrators

Amazon Web Services EMEA SARL – Amazon Bedrock Runtime · optional/conditional

Subject matter of service	Provision of selected Anthropic models
Data processed	Prompts, required workspace context and generated outputs
Location of processing	European Union: Germany (eu-central-1), Ireland (eu-west-1), France (eu-west-3), Sweden (eu-north-1), Italy (eu-south-1) and Spain (eu-south-2). Inference requests may be processed within these AWS regions; no global processing takes place.
Storage and training	No storage of inference data at the model inference service and no training of general models. Chat histories remain in the awork Azure infrastructure.
Safeguards and controls	- Data processing agreement with Amazon Web Services - Encrypted transmission of data - Exclusive use of geographically restricted EU inference profiles - No access by the model providers to prompts or model outputs - Use of the models provided via AWS can be deactivated per workspace by administrators - Security and content filters via Amazon Bedrock Guardrails

TensorX Limited · optional/conditional

Subject matter of service	Provision of selected open-source AI models, currently Qwen, GLM, Kimi and DeepSeek
Data processed	Prompts, required workspace context and generated outputs
Location of processing	Exclusively within the EEA on TensorX-owned hardware in Dublin, Ireland, and Helsinki, Finland
Storage and training	No storage or logging of prompts and model outputs; no use for training purposes; processing of inference data exclusively in volatile memory on TensorX-owned hardware; no disclosure to model providers
Safeguards and controls	- Data processing agreement with TensorX - Processing exclusively in volatile memory on own hardware - No disclosure of inference data to the model providers

OpenAI Ireland Ltd. – OpenAI API / AI model inference · optional/conditional

Subject matter of service	Provision of selected AI models for AI functions in awork AI.
Data processed	Prompts, required selected content and workspace context, and generated outputs, insofar as the respective function uses OpenAI.
Location of processing	Processing of customer content via the European processing region agreed and configured for the deployment. The geographic requirements and, where applicable, safeguards for third-country processing are governed by the applicable data processing agreement with OpenAI and the activated processing settings.
Storage and training	No use of customer content transmitted for model inference to train general models. For the API processing used, zero data retention and the required regional processing settings have been agreed and activated; technically necessary or contractually permitted exceptions remain unaffected in accordance with the applicable provider terms.
Safeguards	Data processing agreement with OpenAI, encryption in transit, technical access controls, and agreed regional processing and retention settings.

ANNEX 2 – PERSONS AUTHORISED TO ISSUE INSTRUCTIONS

2.1 PERSONS AUTHORISED TO ISSUE INSTRUCTIONS ON BEHALF OF THE CUSTOMER

Instructions may only be issued by persons who represent the Customer in this respect by virtue of their corporate position or their particular function (e.g. data protection officer, chief security officer, etc.).

2.2 RECIPIENTS OF INSTRUCTIONS AT THE PROCESSOR

Lucas Bauche, Managing Director · Nils Czernig and Tobias Hagenau, Managing Directors · Communication channel: privacy@awork.com

ANNEX 3 – DATA PROTECTION OFFICER

PROLIANCE GmbH · www.proliance.ai · Leopoldstraße 21 · 80802 Munich, Germany · datenschutzbeauftragter@proliance.ai

ANNEX 4 – TECHNICAL AND ORGANISATIONAL MEASURES

4.1 PHYSICAL ACCESS CONTROL TO PREMISES AND FACILITIES IN WHICH DATA IS PROCESSED

a) Access to the Processor's premises used to perform the order is restricted to the persons required to perform the order.

b) The entrances to the Processor's premises in which personal data is processed are secured against unauthorised access by security locks or magnetic card locks.

c) The issuance of keys and access cards is logged.

d) Doors, gates and windows of the Processor's premises in which personal data is processed are firmly locked outside business hours; doors, gates and windows in the basement and ground floor, as well as all other easily accessible entrances to these rooms, are designed in such a way that they are accessible to unauthorised persons only with considerable difficulty, for example through burglar-resistant doors, gates, windows and locks and/or the use of an intruder alarm system, as well as the security measures of security class SG1 described in VdS 2333.

e) Servers used by the Processor to perform the order are housed in a separately secured server room or data centre, which is additionally secured against unauthorised access by an access control system corresponding to class B under VdS 2367. These rooms are protected against burglary and are constructed at least in accordance with the requirements of security class SG1 under VdS 2333. Access to these premises is limited to the roles and persons required for maintenance and repair and otherwise specifically required.

4.2 SYSTEM ACCESS CONTROL

a) The information processing systems (client and server systems) used by the Processor to perform the order are protected by authentication and authorisation systems.

b) Identification and authentication information (in particular in the form of user names and passwords) associated with access authorisation to the information processing systems used to perform the order is issued only to the persons commissioned to perform the order and only to the extent required for the respective task.

c) Every grant of access authorisation is documented for the duration of the order.

d) All accesses and identifiers ("accounts") are issued exclusively on a person-specific basis. The use of accounts by several persons (group accounts) is in principle not permitted.

e) Identification and authentication information is used exclusively by the individual concerned; a password contained in such information is issued as an initial password and, in accordance with the provisions set out in this Annex, is changed without undue delay after receipt by the authorised person to a password known only to the authorised person; any disclosure is prohibited. If unauthorised persons gain knowledge of access data, the Processor shall notify the controller without undue delay.

f) Passwords are chosen with sufficient complexity and quality. Sufficient complexity and quality means a length of at least ten (10) characters using three of the following 4 categories (upper- and lower-

case letters, digits and special characters), no use of generic terms or proper names, and the non-admissibility of at least the last three (3) passwords used.

g) The Processor keeps authentication data (in particular passwords and cryptographic keys) strictly secret from unauthorised persons, does not store it in plain text and uses it exclusively with encryption in accordance with this Annex or as an irreversible cryptographic checksum (in particular for storage and transmission over the network).

h) The AES algorithm with 256 bits is used for encryption and the HMAC algorithm with 512 bits for password hashes.

i) Every issuance of hardware to employees of the Processor is documented for the duration of the order.

4.3 DATA ACCESS CONTROL

a) Where personal data is stored on the Processor's information processing systems to perform the order, a graded and suitably granular permission system has been set up and technically implemented for all access to personal data. This ensures that access rights are designed in such a way that they allow only the employees engaged in providing the services to access the personal data, in each case to the extent necessary to perform their specific tasks. The assignment of administrator rights to employees of the Processor is limited to the absolutely necessary extent.

b) All processed data is transmitted in encrypted form. All personal data is stored in encrypted form in our database systems. Every access likewise takes place via encrypted data channels.

c) Where personal data is stored on the Processor's information processing systems, all access to personal data (including read, modify and delete access) is logged by user, date, time and the personal data concerned for at least 90 days.

d) All end devices used in the course of the processing (laptops, telephones, etc.) are equipped with an automatic screen lock upon inactivity.

e) A clean desk policy applies in the Processor's premises; desks and other surfaces are to be left free of any documents.

4.4 INPUT CONTROL

a) The entry, modification and deletion of data in the server systems used is logged automatically.

b) The entry, modification and deletion of data in the server systems used is traceable through the use of individual user names.

c) Rights to enter, modify and delete data in the server systems used are assigned on the basis of an authorisation concept.

d) Files and documents are stored in document management systems that automatically log entries and changes with date and user ID.

e) Before new programs and updates are installed on the server systems used, their integrity is ensured by functional tests.

4.5 ORDER CONTROL

a) The persons employed by the Processor to perform the order are comprehensively trained on the general principles and on the specific data protection requirements arising from this DPA, including data security, before they are deployed at the Processor to perform the order, and regularly thereafter.

b) At the end of, and on the basis of, the training process set out in a) of this Section, the persons employed by the Processor to perform the order are bound to confidentiality and to the protection of personal data. This obligation extends to telecommunications secrecy and the associated principles and requirements for the confidentiality of telecommunications, where this is required under the specific order, in particular where the order involves access to traffic data.

c) Orders are awarded to sub-processors exclusively in writing, after conclusion of a data processing agreement and after thorough review of the technical and organisational measures established at the sub-processor.

d) A central register of all data processing agreements concluded with the sub-processors engaged is maintained.

e) After the end of the cooperation with sub-processors, they are instructed to properly delete all processed personal data.

4.6 SEPARATE PROCESSING OF DATA / SEPARATION CONTROL

a) Where personal data is stored on the Processor's information processing systems, complete separation of the personal data from personal data of other customers is implemented, thereby ensuring that personal data can be identified and deleted completely at any time, e.g. by storing the personal data in a separate tenant, in a separate partition or retrievable separately under unique identifiers.

b) Corresponding separation is also implemented for personal data itself if it is stored for different purposes.

4.7 TRANSFER CONTROL

a) Personal data cannot be copied (in particular saved to external data carriers), disclosed and/or deleted without authorisation.

b) Data carriers and all documents, insofar as they contain personal data (including all backup copies of personal data that may exist and copies of original documents), are kept in properly locked data backup cabinets used exclusively for performing the order, if and as long as they are not being processed in accordance with this Annex.

c) Original documents containing personal data are handed out by the persons responsible for managing the process to the persons engaged in providing the services and are taken back by them after the end of work.

d) The persons employed in performing the order are permitted to make handwritten notes only to the extent necessary for providing the services and on specially marked work materials (e.g. paginated or coloured paper).

e) Original documents issued in accordance with this Annex or handwritten notes created in accordance with this Annex are protected against unauthorised access even when the workplace is left only briefly ("Clean Desk Policy").

f) The persons employed by the Processor in performing the order use client systems that are adequately secured. All client systems are equipped with a firewall and virus protection and are regularly checked against common security standards.

g) On server systems with non-volatile memory used by the Processor to perform the order, e.g. network printers or scanners, personal data is not stored beyond the extent directly required for performing the contract. Where third parties are entrusted with the maintenance of such systems, Section 5.3 of this Annex applies accordingly.

h) Wi-Fi access points for network access provided on the Customer's premises are encrypted.

i) If, under the order, the Processor is obliged to delete personal data, the Processor shall

i. carry out the data-protection-compliant, non-recoverable deletion of all deletable electronic data carriers containing personal data (in particular hard drives, USB sticks, floppy disks, tapes);

ii. achieve the lasting and irreversible removal of personal data from database or file systems and from all other deletable storage media;

iii. destroy all paper documents containing personal data and other data carriers that cannot be deleted in accordance with (i) or (ii) of this Section (including all misprints containing personal data, memory cards, USB sticks, etc.) using a commercially available document shredder in accordance with security level 3 under DIN standard 32757 or an at least equivalent method, whereby defective magnetic data carriers that cannot be mechanically destroyed as stated above (e.g. defective hard drives) are to be erased using an approved erasing device in accordance with DIN 33858;

iv. log the deletion for the duration of the order.

4.8 AVAILABILITY AND RESILIENCE (ART. 32(1)(b) GDPR)

a) Server systems used by the Processor to perform the order are protected by firewalls, which secure these server systems against access that is not operationally necessary.

b) All software used, where applicable, by the Processor to perform the order is kept up to date, and security-relevant updates (in particular updates, patches, fixes) are installed without undue delay after they have been made generally available by the software manufacturer and tested by the Processor using a procedure that reflects the state of the art. For updates classified as "critical" or equivalent, the period under sentence 1 is a maximum of two (2) days.

c) Original documents containing personal data, as well as personal data lawfully stored on information processing systems at the Processor, are protected by technical and organisational measures against loss through accidental, negligent or intentional deletion or alteration.

d) Backup copies of personal data lawfully stored on information processing systems at the Processor are treated in accordance with the same requirements as original data, in particular secured against unauthorised access.

e) All server systems used are equipped with fire and smoke detection systems, fire extinguishing systems, air-conditioned server rooms, protective measures against overvoltage, video surveillance and alarm systems for unauthorised access to the server room.

f) All storage systems have redundant storage media (e.g. RAID systems, mirroring or comparable).

g) The Processor has a backup and recovery concept that enables the restoration of backups from the last 30 days.

h) Data storage takes place separately from the storage of operating and application systems.

i) Data and backups are stored in at least two separate fire protection zones.

j) Data recovery is tested regularly and the test result is logged.

4.9 DATA PROTECTION BY DESIGN AND BY DEFAULT

a) No more personal data is collected than is necessary for the respective purpose.

b) Suitable technical measures (independent initiation and confirmation of the deletion process) ensure that data subjects can easily exercise their right of withdrawal.

4.10 ORGANISATIONAL CONTROL

a) The Processor appoints an external data protection officer.

b) The appointed data protection officer is supported in his or her work by an internal employee ("Lead Function Data Protection").

c) All employees of the Processor are trained in data protection matters and the data protection concepts in place at least once a year. Training materials are available in writing and as training videos.

d) Internal policies and work instructions apply to employees of the Processor on a. handling of personal data when working from home / mobile working, b. use of the company internet access and company email accounts, c. use of private devices for business activities (bring your own device).

e) All employees of the Processor are bound in writing to data protection confidentiality.

4.11 REGULAR REVIEW AND EFFECTIVENESS CHECKS

a) The measures listed in this Annex are reviewed at least once a year by the management and the head of IT in cooperation with the data protection officer.

b) If the review establishes that technological standards or organisational processes have changed and such changes make an adjustment of the measures listed here necessary, the adjustments required as a result are implemented without undue delay. The principle of proportionality is observed in doing so.

c) Changes are also made on an ad hoc basis where this is necessary for security reasons.

d) The review and any resulting changes are documented and filed.