DATA PROCESSING AGREEMENT ("DPA")

pursuant to Art. 28 GDPR

between

Users of the web application awork

– hereinafter referred to as the "Controller" –

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 the "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 to establish the data protection framework for the contractual relationship between the parties.

1.2 The description of the respective assignment, including details of its subject matter, the scope, nature and purpose of the data processing, the type of personal data and the categories of data subjects, is set out in section 1 of the Annex.

2. PLACE OF DATA PROCESSING

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

2.2 The Processor may process Controller data through entities outside the Safe Countries ("Third Country"), or have such data processed there, 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 takes place on the basis of and in accordance with the EU Standard Contractual Clauses ("SCC") applicable from time to time, which are to be submitted to the Controller and agreed in writing with the entity established in the Third Country ("data importer"). Where the data importer and the Processor are not identical, the Processor must accede to those SCC. The provisions laid down 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. To the extent that, at the time of termination, one or more main agreements under which the Processor processes personal data of the Controller on its behalf are still in force, the provisions of this agreement continue to apply until the regular expiry of the main agreement(s).

3.2 The Controller may terminate this agreement without notice in the event of a serious breach by the Processor of data protection provisions 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 Controller. This does not apply to the extent that the Processor is required to process the data under EU or member state law to which the Processor is subject. In that case the Processor notifies the Controller of those legal requirements prior to processing, unless such notification is prohibited by the law in question on important grounds of public interest.

4.2 Where instructions amend, revoke or supplement the specifications set out in section 1 of the Annex to this agreement, they are permissible only if a corresponding new agreement is concluded in writing.

4.3 Irrespective of the form in which they are issued, both the Processor and the Controller document every instruction of the Controller in text form. Instructions must be retained for the term of this agreement and for a further three years thereafter.

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

4.5 Instructions may only be issued by persons who, by virtue of their corporate position or their particular function, represent the Controller in this respect (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 of contact persons or their prolonged unavailability, the successors or deputies must be notified to the contractual partner without undue delay in written or electronic form.

5. THE PROCESSOR'S DUTIES TO PROVIDE ASSISTANCE

5.1 Taking into account the nature of the processing, the Processor implements appropriate technical and organisational measures to assist the Controller in fulfilling its obligation to respond to requests from data subjects pursuant to Art. 12 to 22 GDPR.

5.2 Taking into account the nature of the processing and the information available to it, the Processor assists the controller in complying with its obligations under Art. 32 to 36 GDPR. Specifically, with the security of processing, notifications of breaches to the supervisory authority, the communication of a breach to data subjects, data protection impact assessments and consultation of the competent supervisory authority.

5.3 Where 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 informs the Controller thereof without undue delay and coordinates the further steps with it.

6. THE CONTROLLER'S AUDIT RIGHTS

6.1 Upon the Controller's request, the Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations set out in this agreement and in Art. 28 GDPR. In particular, the Processor provides the Controller with information about the data stored and the data processing programmes.

6.2 The Controller or third parties commissioned by it are entitled – generally subject to an appointment arranged at least 30 days in advance – to verify compliance with the obligations arising from this agreement and from Art. 28 GDPR and to carry out on-site inspections at the Processor's premises.

The Processor enables and contributes to such inspections. Inspections without specific cause are limited to a maximum of one inspection per year.

6.3 Upon request, the Processor must provide the Controller with suitable evidence of compliance with the obligations under Art. 28(1) and (4) GDPR. Such evidence may be provided by making available documents and certificates reflecting approved codes of conduct within the meaning of Art. 40 GDPR or approved certification mechanisms within the meaning of Art. 42 GDPR.

7. THE PROCESSOR'S DATA PROTECTION OFFICER

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

8. CONFIDENTIALITY

8.1 The Processor confirms that it is aware of the data protection provisions of the GDPR relevant to processing on behalf of a controller. When processing the Controller's personal data, it observes data secrecy and confidentiality. This obligation continues to apply after the termination of this contractual relationship.

8.2 The Processor warrants that it familiarises the employees engaged in performing the work with the data protection provisions applicable to them. It obliges these employees by written agreement to maintain confidentiality both for the duration of their activity and after the end of their employment relationship, unless they are subject to an appropriate statutory duty of confidentiality. The Processor monitors compliance with data protection provisions within its organisation.

8.3 The Processor may provide information to third parties or data subjects only with the prior written consent, or consent in an electronic format, of the Controller. 9. TECHNICAL AND ORGANISATIONAL MEASURES

9.1 The Processor implements appropriate technical and organisational measures in such a way that the processing complies with the requirements of the GDPR and that the protection of the rights of the data subject is ensured. It structures its internal organisation so as to meet the specific requirements of data protection and to achieve an appropriate level of protection. In particular, taking into account the state of the art, the Processor must ensure the appropriate security of the processing, in particular the confidentiality (including pseudonymisation and encryption), availability, integrity and resilience of the systems and services used for the data processing.

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

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

10. THE PROCESSOR'S INFORMATION OBLIGATIONS AND PERSONAL DATA BREACHES

10.1 The Processor informs the Controller 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 assists the Controller in investigating, mitigating and remedying the breaches.

10.3 Should the personal data processed under this agreement be endangered at the Processor by seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties, the Processor must inform the Controller thereof without undue delay. The Processor will also inform all relevant bodies in this context without undue delay that control over the data lies with the Controller.

10.4 Where inspections by data protection supervisory authorities are carried out, the Processor undertakes to disclose the outcome to the Controller to the extent that it concerns the processing of personal data under this agreement. The Processor will remedy the deficiencies identified in the inspection report without undue delay and inform the Controller thereof.

11. SUBPROCESSORS

11.1 The Controller authorises the Processor to involve subcontractors in the processing. Separate prior consent by the Controller is not required. The Processor informs the Controller in text form of any intended change concerning the engagement or replacement of a subcontractor at least 6 weeks before the planned change. The Controller may object to the change in text form within 3 weeks of receiving the information, for good cause. An objection gives rise to a mutual right of extraordinary termination of the main agreement. If no objection is raised within the period, consent is deemed granted.

11.2 The Processor must ensure contractually that the provisions agreed in this agreement also apply vis-à-vis subprocessors. The Processor's contract with the subcontractor must be concluded in writing or in electronic format.

11.3 Subcontractors in third countries are engaged only if the special requirements of Art. 44 et seq. GDPR are met.

11.4 The Controller hereby also expressly consents to the engagement of the subprocessors listed in the Annex.

11.5 The Processor ensures that the Controller has the same rights of instruction and control vis-à-vis the subprocessor as it has vis-à-vis the Processor under this agreement. Where a subprocessor fails to comply with its data protection obligations, the Processor is liable to the Controller for that subprocessor's performance of its obligations.

11.6 At the Controller's request, the Processor must provide the Controller with evidence of the conclusion of the agreements entered into with the subcontractor. Such evidence must 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, within 35 days, all personal data received in the course of the processing. This includes in particular the results of the data processing, documents provided, data carriers provided and copies of the personal data. The obligation to delete does not apply where the Processor is legally required under EU or member state law to continue storing the data. If a further storage obligation exists, the Processor must restrict the processing of the personal data and use the data only for the purposes for which a storage obligation exists. The obligations regarding the security of

processing continue to apply for the period of storage. The Processor must delete the data within 35 days as soon as the storage obligation ceases to apply. Note: Deletion within less than 35 days is not technically possible due to the established backup concept of the databases used.

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

12.3 The operations must be logged with an indication of the date.

12.4 At the Controller's request, personal data received by the Processor from the Controller in the course of the processing will be returned to the Controller within 35 days upon 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 Controller only for fault within its own 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 respect to the data processed for the Controller.

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

14.3 Amendments or ancillary agreements require written form or an electronic format. This also applies to any amendment of this form requirement.

14.4 To the extent that agreements on data processing on behalf of a controller already exist between the parties with respect to the services set out in or referred to by this DPA, those agreements are superseded upon this DPA taking effect, and this DPA conclusively governs the parties' rights and obligations 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 each of them in electronic form as a PDF. Signing may also take place through the Processor's digital online registration process. The Controller warrants that the person signing or completing the online registration process (authorised representative) holds all powers of attorney and authorisations required to conclude this DPA. The Controller will be bound by all declarations made by the authorised representative. Amendments to this DPA, including its annexes, are likewise subject to the form requirements set out in this section.

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

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

ANNEX TO THE DATA PROCESSING AGREEMENT

1. SUBJECT MATTER OF THE ASSIGNMENT

1.1 SUBJECT MATTER OF THE ASSIGNMENT

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

1.2 SCOPE, NATURE (ART. 4 NO. 2 GDPR) AND PURPOSE OF THE DATA PROCESSING

Personal data is processed for the purpose of providing the software-as-a-service application awork, by means of which the Controller's work, team and project organisation is carried out. This means in particular:

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

For this purpose, personal data is recorded, stored, read, organised and structured, displayed in user interfaces and deleted.

1.2.1 SUPPLEMENTARY OPTIONAL AI PROCESSING · NEW IN V05

To the extent that AI-supported functions are available in the booked awork plan or in the awork AI add-on, 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 Controller 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 within the Azure infrastructure controlled by awork, so that this content can be displayed in the product
- execution of agents, tools, connections, triggers and schedules within the permissions granted by the Controller
- no use of Controller data for training general models and no storage of prompts or outputs by the model inference providers engaged
- no use of AWS Bedrock as a failover or peak-load fallback for the regular Azure-based AI processing

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

1.3 CATEGORIES OF DATA SUBJECTS AND TYPES OF DATA

Personal data relating to the following groups of persons is collected, processed and used, provided that this is necessary to fulfil the stated purpose:

- Internal and external staff (e.g. freelancers) and temporary staff of the Controller
    - Professional contact and (work) organisation data for the administration of users: surname, first name, gender, e-mail, 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 Controller
    - Professional contact and (work) organisation data: surname, first name, e-mail, telephone number
- Additionally, when using optional AI functions
    - content from prompts, selected workspace context, documents and files as well as model outputs
    - agent configurations, tool calls and agent/tool activity information
    - Other personal data that the Controller releases for processing; special categories pursuant to Art. 9 GDPR only to the extent that the Controller enters or releases such data on its own responsibility

2. PERSONS AUTHORISED TO ISSUE INSTRUCTIONS

2.1 PERSONS OF THE CONTROLLER AUTHORISED TO ISSUE INSTRUCTIONS

Instructions may only be issued by persons who, by virtue of their corporate position or their particular function, represent the Controller in this respect (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

3. DATA PROTECTION OFFICER

PROLIANCE GmbH · www.datenschutzexperte.de · Leopoldstraße 21 · 80802 Munich, Germany · datenschutzbeauftragter@datenschutzexperte.de

ANNEX: LIST OF SUBPROCESSORS

The awork application can be used without AI data processing; AI functions of the standard product can be deactivated by the administrator, and the awork AI add-on requires a separate booking. Providers designated as optional or conditional are engaged only if the designated function or model is available and activated for the workspace.

A. GENERAL PLATFORM SERVICES

Microsoft Ireland Operations Limited – Azure Compute/Storage

Subject matter of the service	Primary hosting. Provision of the technical infrastructure for operating awork in German data centres; includes servers, storage space and network services.
Data processed	All data referred to in Annex 1.2; all data entered in awork, e.g. projects, tasks, time tracking 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.
Protective measures	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 the service	Fast and secure delivery of the awork application via a global content delivery network as well as protection against cyber attacks.
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 where access takes place from a non-EU country may a technically necessary, short-term processing of technical connection data occur via the geographically nearest server; stored content is not affected by this.
Protective measures	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; where technically necessary third-country processing occurs, an adequacy decision or SCC apply.

Birdie.so / Philo Labs

Subject matter of the service	Tool for capturing and reporting errors. Only becomes active if a user reports a bug themselves using a screen recording; captures technical context information to enable 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 e-mail for responses.
Location	EU: Paris, France.
Protective measures	DPA with guaranteed exclusive EU processing; no third-country transfer; encrypted data transmission; data minimisation to bug-relevant information; automatic deletion 90 days after the ticket has been processed. Business data is not transmitted automatically.

Twilio Ireland Limited – Segment

Subject matter of the service	Exclusively technical forwarding of 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 as well as, where applicable, support-related content submitted by the user
Location	primarily EU: processing in the USA within the Twilio infrastructure possible
Protective measures	DPA; EU-US Data Privacy Framework; SCC as additional safeguard; data minimisation

Intercom, Inc.

Subject matter of the service	Customer support and support communication in awork
Data processed	In the case of support contact: a) name, e-mail, chat history b) content shared by the user (e.g. screenshots) In the case of system messages: a) e-mail address for important updates
Location	USA
Protective measures	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 the service	AI functions in the standard product and in the awork AI add-on
Data processed	Prompts, required workspace context and generated text or image outputs
Place 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.
Protective measures and controls	- Data processing agreement with Microsoft - Encrypted transmission of the data - Integrated security and content filters - Use of the 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 the service	Provision of selected Google/Gemini text and image models
Data processed	Prompts, required workspace context and generated outputs
Place 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.
Protective measures and controls	- Data processing agreement with Google - Encrypted transmission of the data - Processing in the designated Google Cloud region in Belgium - Integrated and configurable security filters check inputs and outputs for harmful content and can block such content - 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 the service	Provision of selected Anthropic models
Data processed	Prompts, required workspace context and generated outputs

Place 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; global processing does not take 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.
Protective measures and controls	- Data processing agreement with Amazon Web Services - Encrypted transmission of the 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 the service	Provision of selected open-source AI models, currently Qwen, GLM, Kimi and DeepSeek
Data processed	Prompts, required workspace context and generated outputs
Place 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
Protective measures and controls	- Data processing agreement with TensorX - Processing exclusively in volatile memory on own hardware - No disclosure of the inference data to the model providers

4. TECHNICAL AND ORGANISATIONAL MEASURES

Adopted unchanged from V04.

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 for performing the assignment is limited to those persons necessary for performing the assignment.

b) The entrances to the Processor's premises in which personal data is processed are secured against access by unauthorised persons with security 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 securely locked outside business hours; doors, gates and windows in the basement and on the ground floor as well as all other easily accessible entrances to these rooms are designed such that they are considerably more difficult for unauthorised persons to access, for instance 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 assignment are housed in a separately secured server room or data centre which is specifically protected against access by unauthorised persons by an access control system in accordance with class B pursuant to VdS 2367. These rooms are burglar-resistant and designed at least in accordance with the requirements of security class SG1 pursuant to VdS 2333. Access to these premises is limited to the roles and persons specifically required for maintenance and repair and otherwise.

4.2 SYSTEM ACCESS CONTROL

a) The information processing systems (client and server systems) used by the processor to perform the assignment 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 assignment is issued only to the persons entrusted with performing the assignment and only to the extent required for the respective task.

c) Every issuance of access authorisations is documented for the term of the assignment.

d) All access rights and identifiers (“accounts”) are issued on a person-specific basis only. The use of accounts by several persons (group accounts) is generally not permitted.

e) Identification and authentication information is used personally only; any password contained in such information is issued as an initial password and is changed without undue delay upon receipt by the authorised person, in accordance with the provisions set out in this annex, to a password known only to the authorised person; it must not be passed on. If unauthorised persons obtain knowledge of access credentials, the processor notifies the controller thereof without undue delay.

f) Passwords are chosen with sufficient complexity and quality. Sufficient complexity and quality means a minimum length of 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 inadmissibility 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 corresponding to this annex or as an irreversible cryptographic checksum (in particular for storage and transmission over the network).

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

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

4.3 DATA ACCESS CONTROL

a) Where personal data is stored on the processor's information processing systems for the purpose of performing the assignment, a graduated and suitably granular permissions system is set up and technically implemented for all access to personal data. This ensures that access rights are designed such that they allow the employees deployed for the provision of services access to the personal data only to the extent necessary for performing the specific tasks. The granting of administrator rights is limited to the strictly necessary number of the processor's employees.

b) All data processed is transmitted in encrypted form. All personal data is stored in encrypted form in our database systems. All 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 in each case for at least 90 days.

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

e) A clean desk policy applies on the Processor's premises; desks and other surfaces must 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 granted on the basis of an authorisation concept.

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

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

4.5 ASSIGNMENT CONTROL

a) The persons employed by the processor to perform the assignment receive comprehensive training on the general principles as well as on the specific data protection requirements arising from this DPA, including data security, before being deployed by the processor to perform the assignment and at regular intervals 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 assignment are placed under an obligation of confidentiality and protection of personal data. This obligation extends to the secrecy of telecommunications and the associated principles and requirements regarding the confidentiality of telecommunications where this is required under the specific assignment, in particular where the assignment involves access to traffic data.

c) Assignments are awarded to subprocessors exclusively in writing, following the conclusion of a data processing agreement and a thorough review of the technical and organisational measures established at the subprocessor.

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

e) Upon termination of the cooperation with subprocessors, they are instructed to properly delete all personal data processed.

4.6 SEPARATE PROCESSING OF DATA/SEPARATION CONTROL

a) Where personal data is stored on the processor's information processing systems, a complete separation of the personal data from personal data of other controllers 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 dedicated tenant, in a dedicated partition or retrievable separately under a unique identifier.

b) A corresponding separation is also implemented for personal data itself where 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 as well as all documents containing personal data (including any backup copies of personal data and copies of original documents) are kept in properly locked data security cabinets used exclusively for performing the assignment, if and for as long as they are not being processed in accordance with this annex.

c) Original documents containing personal data are to be issued by the persons responsible for managing the process to the persons deployed for the provision of services and taken back from them at the end of work.

d) The persons employed in performing the assignment are permitted to make handwritten notes only to the extent necessary for the provision of services and on specially marked working 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, including where the workplace is left only briefly (“clean desk policy”).

f) The persons employed by the processor in performing the assignment use client systems that are sufficiently 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 assignment, e.g. network printers or scanners, personal data is not stored beyond the extent directly necessary for performing the contract. Where third parties are entrusted with the maintenance of such systems, section 5.3 of this annex applies accordingly.

h) WLAN access provided on the Controller's premises for network access is encrypted.

i) Where the processor is under an obligation to delete personal data in accordance with the assignment, the processor will

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

ii. implement the permanent and irreversible removal of personal data from database or file systems as well as from all other erasable storage media;

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

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

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

a) Server systems used by the processor to perform the assignment are protected by firewalls which secure these server systems against access not necessary for operations.

b) All software used by the Processor to perform the assignment, if any, 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 under a procedure corresponding to the state of the art. For updates qualified as “critical” or similar, 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 against loss by accidental, negligent or intentional deletion or alteration by means of technical and organisational measures.

d) Backup copies of personal data lawfully stored on information processing systems at the Processor are treated according to the same standards 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 as well as alarm systems for unauthorised entry 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 restoration is tested regularly and the test result is logged.

4.9 DATA-PROTECTION-FRIENDLY DEFAULT SETTINGS, PRIVACY BY DEFAULT

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

b) Appropriate 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) An external data protection officer is appointed by the Processor.

b) The appointed data protection officer is supported in their work by an internal employee (“data protection lead function”).

c) All employees of the Processor receive training on data protection matters and the existing data protection concepts at least once a year. Training materials are available in written form and as training videos.

d) Internal guidelines and work instructions apply to employees of the Processor concerning a. handling of personal data in the home office / mobile office, b. use of the company internet access and the company e-mail account, c. use of private devices for company activities (bring your own device).

e) All employees of the Processor are placed under a written obligation of data protection confidentiality.

4.11 REGULAR REVIEW AND EFFECTIVENESS ASSESSMENT

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

b) In the event that the review establishes that technological standards or organisational processes have changed and that such changes make an adaptation of the measures listed here necessary, the resulting necessary adaptations are implemented without undue delay. The principle of proportionality is observed in this respect.

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.