DATA PROCESSING AGREEMENT ("DPA")

PURSUANT TO ART. 28 GDPR

between

users of the awork web application

– hereinafter referred to as the "Client" –

and the data processor

awork GmbH

Großer Burstah 36/38

20457 Hamburg

– hereinafter referred to as the "Contractor" –

– hereinafter collectively referred to as the "Parties" –

PREAMBLE

The terms and definitions of Regulation (EU) 2016/679 (hereinafter referred to as "GDPR"), in particular Art. 4 GDPR, apply to this data processing agreement.

1. SUBJECT

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 order with details of the subject matter of the order, scope, type and purpose of data processing, type of personal data and categories of data subjects can be found in the appendix under section 1.

2. PLACE OF DATA PROCESSING

2.1 The contractually agreed processing shall take place in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another contracting state of the Agreement on the European Economic Area ("Safe Countries"), unless otherwise specified in the Annex.

2.2 The contractor may only process or have processed client data by entities outside the Safe States ("third country") if and to the extent that (i) an adequate level of data protection has been established for the third country in question on the basis of a valid decision by 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 must be submitted to the Client and agreed in writing with the entity based in the third country ("data importer"). If the data importer and the Contractor are not identical, the Contractor must accede to these SCC. The provisions set out in these GTC remain unaffected.

3. TERM

3.1 This contract 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 contracts are still in force under which the contractor processes personal data of the client on behalf of the client, the provisions of this contract shall continue to apply until the regular termination of the main contract(s).

3.2 The client may terminate this contract without notice if the contractor commits a serious breach of data protection regulations or the provisions of this contract. In particular, failure to comply with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a serious breach.

4. INSTRUCTION

4.1 The contractor shall process the personal data only within the scope of the instructions issued by the client. This shall not apply if the contractor is obliged to process the data by EU law or the law of the Member States to which the contractor is subject. In this case, the contractor shall notify the client of these legal requirements prior to processing, unless such notification is prohibited by the relevant law on grounds of an important public interest.

4.2 If instructions change, cancel or supplement the provisions set out in clause 1 of the annex to this contract, they shall only be permissible if a corresponding new agreement is made in writing.

4.3 Regardless of the form in which instructions are issued, both the contractor and the client shall document each instruction from the client in writing. The instructions shall be retained for the duration of this contract and for a further three years thereafter.

4.4 The contractor shall immediately notify the client if, in its opinion, an instruction issued by the client violates legal regulations. In such a case, the contractor is entitled, after timely notification to , to suspend the execution of the instruction until the client has changed or confirmed the instruction. If the contractor can demonstrate that processing in accordance with the client's

instructions may lead to liability on the part of the contractor under Art. 82 GDPR, the contractor shall be free to suspend further processing in this respect until the liability between the parties has been clarified.

4.5 Instructions may only be issued by persons who, due to their institutional position or special function, represent the client in this respect (e.g. data protection officer, chief security officer, etc.).

4.6 The contractor shall specify the persons receiving instructions in the annex to this contract. In the event of a change or long-term absence of the contact persons, the contractual partner shall be notified immediately and in writing or electronic form of the successors or representatives.

5. SUPPORT OBLIGATIONS OF THE CONTRACTOR

5.1 In view of the nature of the processing, the contractor shall take appropriate technical and organisational measures to support the client in its obligation to respond to requests from data subjects in accordance with Articles 12 to 22 of the GDPR.

5.2 Taking into account the nature of the processing and the information available to it, the contractor shall support the controller in complying with its obligations under Articles 32 to 36 GDPR. In particular, this applies to the security of processing, reporting breaches to the supervisory authority, notifying data subjects in the event of a breach, data protection impact assessments and consulting the competent supervisory authority.

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

6. RIGHTS OF INSPECTION OF THE CLIENT

6.1 Upon request, the contractor shall provide the client with all necessary information to prove compliance with the obligations set out in this contract and Art. 28 GDPR. In particular, the contractor shall provide the client with information about the stored data and the data processing programmes.

6.2 The client or third parties commissioned by it shall be entitled – in principle by appointment at least 30 days in advance – to check compliance with the obligations under this contract and Art. 28 GDPR and to carry out on-site inspections at the contractor's premises. The contractor shall facilitate and contribute to this. Unannounced inspections shall be limited to a maximum of one inspection per year.

6.3 Upon request, the contractor shall provide the client with suitable evidence of compliance with the obligations under Art. 28(1) and (4) GDPR. This proof may be provided by means of documents and certificates reflecting 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 CONTRACTOR

7.1 The data protection officer of the contractor is listed in the appendix to this contract under section 3.

8. CONFIDENTIALITY

8.1 The contractor confirms that it is familiar with the relevant data protection provisions of the GDPR applicable to order processing. It shall maintain data secrecy and confidentiality when processing the client's personal data. This obligation shall continue to apply even after the termination of this contractual relationship.

8.2 The contractor assures that it will familiarise the employees involved in carrying out the work with the relevant data protection provisions. It shall oblige these employees by written agreement to maintain confidentiality for the duration of their employment and also after termination of the employment relationship, unless they are subject to an appropriate statutory duty of confidentiality. The contractor shall monitor compliance with data protection regulations within its company.

8.3 The contractor may only disclose information to third parties or data subjects with the prior written consent or consent in electronic format of the client.

9. TECHNICAL AND ORGANISATIONAL MEASURES

9.1 The contractor shall implement appropriate technical and organisational measures to ensure that processing is carried out in accordance with the requirements of the GDPR and that the rights of the data subject are protected. It shall organise its internal operations in such a way that they meet the specific requirements of data protection and achieve an appropriate level of protection. In particular, the contractor shall ensure, taking into account the state of the art, 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 data processing.

9.2 The technical and organisational measures in the annex are defined as binding.

9.3 The technical and organisational measures may be adapted to technical developments during the course of the contractual relationship. In doing so, the adapted measures must at least correspond to the security level of the measures agreed in the annex. Significant changes must be agreed in writing or in electronic format.

10. INFORMATION OBLIGATIONS OF THE CONTRACTOR AND VIOLATION OF THE PROTECTION OF PERSONAL DATA

10.1 The contractor shall immediately inform the client of any breaches or suspected breaches of this contract or regulations concerning the protection of personal data.

10.2 The contractor shall support the client in investigating, mitigating and remedying the breaches.

10.3 If the personal data processed under this agreement is endangered by seizure or confiscation, by insolvency or composition proceedings, or by other events or measures taken by third parties, the contractor shall inform the client immediately. The contractor shall also immediately inform all relevant authorities that the client has control over the data.

10.4 Insofar as audits are carried out by the data protection supervisory authorities, the contractor undertakes to disclose the results to the client insofar as they relate to the processing of personal data under this contract. The contractor shall immediately remedy any deficiencies identified in the audit report and inform the client thereof.

11. SUBCONTRACTORS

11.1 The client authorises the contractor to involve subcontractors in the processing of the order. No separate prior consent from the client is required. The contractor shall inform the client in writing of any intended change with regard to the involvement or replacement of a subcontractor at least 6 weeks before the planned change. The client may object to the change in writing within 3 weeks of receiving the information for good cause. An objection shall result in a mutual, extraordinary right of termination of the main contract. If no objection is made within the deadline, consent shall be deemed to have been given.

11.2 The contractor must contractually ensure that the provisions agreed in this contract also apply to subcontractors. The contractor's contract with the subcontractor must be concluded in writing or in electronic format.

11.3 Subcontractors in third countries may only be commissioned if the special requirements of Art. 44 ff. GDPR are met.

11.4 The client hereby also expressly consents to the commissioning of the subcontractors listed in the appendix.

11.5 The contractor shall ensure that the client has the same rights to issue instructions and exercise control over the subcontractor as it has over the contractor under this contract. If a subcontractor fails to comply with its data protection obligations, the contractor shall be liable to the client for compliance with the obligations of that subcontractor.

11.6 At the request of the client, the contractor shall provide the client with evidence of the agreements concluded with the subcontractor. Such evidence shall be provided in text form.

12. DELETION AND RETURN OF PERSONAL DATA

12.1 After completion of the processing services agreed in the main contract, the contractor is obliged to delete all personal data received in the course of order processing within 35 days. This includes, in particular, the results of data processing, documents and data carriers provided, and copies of personal data. The obligation to delete does not apply if the contractor is legally obliged to continue storing the data under EU or Member State law. If there is a further obligation to store the data, the

contractor must restrict the processing of the personal data and use the data only for the purposes for which there is an obligation to store it. The obligations regarding the security of processing continue to apply for the duration of the storage period. The contractor must delete the data within 35 days as soon as the obligation to store it ceases to apply. Note: Deletion within less than 35 days is technically not possible due to the established backup concept of the databases used.

12.2 The deletion must be carried out in such a way that the data cannot be recovered.

12.3 The processes must be logged with the date.

12.4 At the request of the client, personal data received by the contractor from the client in the course of order processing shall be returned to the client within 35 days after completion of the processing services agreed in the main contract.

13. LIABILITY

13.1 The parties shall be liable in accordance with Art. 82 GDPR.

13.2 In the internal relationship, the contractor shall only be liable to the client for faults within its sphere of influence. The liability provisions of the main contract shall remain unaffected in the internal relationship.

14. FINAL PROVISIONS

14.1 The defence of the 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 client.

14.2 The annex or, in the case of several concluded main contracts, the annexes to this contract are an integral part thereof.

14.3 Any amendments or subsidiary agreements must be made in writing or in electronic format. This also applies to amendments to this formal requirement.

14.4 If agreements on data processing on behalf of the client already exist between the parties with regard to the services specified or referred to in these GTC, these agreements shall be superseded by these GTC upon their entry into force, and these GTC shall conclusively regulate the existing rights and obligations of the parties in this respect.

14.5 The parties agree that these GTC shall be signed by means of an electronic signature and may alternatively be drawn up in writing. They may be validly signed by means of an 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 by means of the contractor's digital online registration process. The client guarantees that the person signing or completing the online registration process (authorised representative) has all the powers of attorney and representation authorisations required to conclude these GTC. The client shall be responsible for all declarations made by the authorised representative. Amendments to these GTC, including their annexes, are also subject to the formal requirements set out in this clause.

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

14.7 These GTC are subject to German law. The place of jurisdiction for disputes arising from these GTC corresponds to the provisions of the main contract.

Appendix to the order processing agreement

1. SUBJECT MATTER OF THE ORDER

1.1 SUBJECT MATTER OF THE CONTRACT:

The processor is a manufacturer and provider of enterprise software for handling all project-related commercial processes. This includes sales, consulting, implementation, integration, hosting and support of the solutions. Data collection, processing and use are carried out for the purposes specified above.

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

Personal data is processed for the purpose of providing the software-as-a-service application awork, which is used to organise the client's work, teams and projects. This means in particular

- hosting (data, application, system, components),
- operation (application, system, components),
- maintenance/support (application, system, components)
- support (application, system, components)
- Further development (application, system, components)

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

1.3 GROUP OF DATA SUBJECTS AND TYPE OF DATA:

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

- **Internal and external employees (e.g. freelancers) & temporary staff of the client:**
  - Professional contact and (work) organisational data for user administration: surname, first name, gender, email address, telephone number, photo
  - Data on professional circumstances: job title, log file information, IP address, working hours, absences, activities
- **Prospective customers, customers and other business partners of the client**
  - Professional contact and (work) organisational data: surname, first name, email address, telephone number

2. PERSONS AUTHORISED TO ISSUE INSTRUCTIONS

2.1 AUTHORISED PERSONS OF THE CLIENT:

Instructions may only be issued by persons who represent the client in this respect due to their institutional position or special function (e.g. data protection officer, chief security officer, etc.).

2.2 PERSONS AUTHORISED TO RECEIVE INSTRUCTIONS AT THE CONTRACTOR ARE:

Name: Bauche, Lucas
Function: Managing Director
Communication channel for instructions: privacy@awork.com

Name: Czernig, Nils and Hagenau, Tobias
Position: Managing Directors
Channel of communication for instructions:privacy@awork.com

3. DATA PROTECTION OFFICER

The contractor's data protection officer is:

EU + European Economic Area
PROLIANCE GmbH
www.datenschutzexperte.de
Leopoldstr. 21
80802 Munich
datenschutzbeauftragter@datenschutzexperte.de

UK
Prighter Ltd
awork ID: 13841150789
https://app.prighter.com/portal/13841150789

awork is registered with ICO **Information Commissioner's Office**
Contact Person for ICO: Jennifer Winter, **Security number:** CSN6055530
Registration reference: ZB867591

Appendix: List of sub-processors

Microsoft Azure – Primary hosting (Germany)

Category	Subcontractor	Subject matter	Processed data	Location of processing/data transfer	Guarantees / protective measures
Hosting (DE)	Microsoft Ireland Operations Limited, Dublin (Azure – Compute/ Storage)	Provision of technical infrastructure for the operation of awork. This includes servers, storage space and network services in German data centres	a) all data mentioned under 1.2 b) all data entered into awork (e.g. projects, tasks, time records, documents) c) user and access authorisations d) uploaded files or content	**Germany only** Data centres: Frankfurt/Main (Germany West Central) and Berlin (Germany North) All customer data is stored and processed exclusively in Germany.	✓Data Processing Agreement (DPA) concluded with Microsoft ✓**Highest security certifications: ISO 27001, SOC 2, BSI C5** ✓Encryption of all data during transmission and storage ✓Strict access controls: awork employees can only access data that they need for their specific tasks (minimum principle) ✓**Guarantee:** No transfer of data outside Germany

Microsoft Azure – Edge delivery & protection (Front Door / CDN)

Category	Subcontractor	Subject matter	Processed data	Location of processing / data transfer	Guarantees / protective measures
Delivery and protection (global)	Microsoft Ireland Operations Limited, Dublin, (Azure Front Door / CDN)	Fast and secure delivery of the awork application through a global network (Content Delivery Network) for short loading times and protection against cyber attacks	a) Technical connection data (IP address, browser information) b) Cached app resources (images, scripts, stylesheets) c) No processing of business data	**Primarily:** EU/Germany Microsoft guarantees that all customer data will be stored and processed exclusively in the region we have selected (EU). **Exception:** Only when accessing awork from a non-EU country may data processing be carried out temporarily via the geographically closest server for technical reasons. This applies to data processing may take place via the geographically closest server. This only applies exclusively to technical processing connection data, not stored content.	✓**Data residency guarantee:** All data remains within the EU. ✓Data Processing Agreement (DPA) concluded with Microsoft ✓Encrypted transmission of all data ✓Technical connection data is stored for a maximum of 30 days ✓No permanent storage of content in the CDN ✓If you are accessing from third countries: adequacy decision or standard contractual clauses apply **Additional note:** The Azure Front Door/CDN system improves the performance of awork without your business data leaving the EU. Data is only transferred to third countries if the user accesses awork from outside the EU.

Microsoft Azure – Optional AI function (Azure OpenAI, EU geography)

Category	Subcontractor	Subject matter	Processed data	Place of processing/data transfer	Guarantees / protective measures
AI (EU)	Microsoft Ireland Operations Limited, Dublin (Azure OpenAI)	**AI-powered assistant features** in awork Intelligent processing and analysis of workspace data to support daily work work (e.g. text generation, summaries, suggestions, automations). **Note:** These functions are enabled by default and only process data for which the user in question has authorisation.	**When enabled** a) Texts and content entered in awork b) Context information from the relevant workspace (only if the appropriate authorisation) c) No permanent storage of the processed content **When deactivated**: no data access / no data processing	Processing in EU data centres (Sweden Central) The data remains entirely within the EU. **Important:** The AI is NOT trained with customer data – content is only processed, not stored or used for training purposes	✓**EU data residency:** No transfer outside the EU ✓Data processing agreement (DPA) concluded with Microsoft ✓**Data protection guarantee:** Your data is NOT used for AI training ✓Integrated content filter blocks abusive or harmful content ✓Data access can be specifically disabled for each workspace ✓Encrypted transmission of all data ✓No logging of content **Additional note for customers:** The AI functions are enabled by default, but can be disabled at any time by the workspace administrator. The AI can only access data for which users already have authorisation. Your business data will never be used to train the AI.

Additional sub-processors

Category	Subcontractor	Subject matter of the contract	Processed data	Place of processing/data transfer	Guarantees / protective measures
CDP/ Events	Twilio Ireland Limited (segment), Dublin	**Technical data forwarding for support functions** Segment forwards technical information to our support system (Intercom) so that we can provide optimal assistance to with any questions.	a) Technical data (e.g. browser used, error messages) User context for b) Support requests (e.g. account information) c) Support content transmitted by the user (e.g. screenshots in chat)	Primarily the EU, but data may also be processed in the USA (Twilio infrastructure)	✓Data processing agreement (DPA) concluded with Twilio ✓Standard contractual clauses (SCC) for secure third-country transfers ✓EU-US Data Privacy Framework (active certification)
Support	Intercom, Inc. USA, San Francisco	**Customer support and help system in awork (including AI-supported support assistant)** a) Live chat for support enquiries c) Help centre with instructions d) Product updates and important system notifications e) Automated assistance	When contacting support: a) Name, email address, chat history b) Content shared by the user (e.g. screenshots) For help centre: a) Technical access data For system messages: a) Email address for important updates	USA	✓Data Processing Agreement (DPA) concluded ✓EU-US Data Privacy Framework (active certification) ✓Standard Contractual Clauses (SCC) as additional security measure ✓Security certifications: ISO 27001, SOC 2 ✓Encrypted data transmission (TLS) ✓Data minimisation: Only support-relevant data **Additional note:** Intercom only becomes active when the user utilises the support chat or accesses help articles. Business data from awork is not automatically transferred to Intercom. The user controls what information they share in support. The AI-powered support assistant analyses questions entered in the chat based on articles from the awork Help Centre.
Bug reporting	Birdie.so (Philo Labs), France, Paris	Tool for error detection and reporting that enables users to report bugs and issues directly from awork, including automatic technical context information for faster problem solving	**Only when bug reporting is active:** a) Error description and comments b) Automatically recorded technical data (browser, operating system, console logs) c) Optional: screenshots or screen recordings (if added by the user) d) Basic user data (name, e-mail) for feedback	Exclusively EU (Paris, France)	✓Data processing agreement (DPA) with guaranteed exclusive EU processing ✓No third country transfer ✓Encrypted data transfer ✓Data minimisation: Only bug-relevant information ✓Automatic deletion after ticket processing after 90 days **Additional note:** Birdie.so only becomes active when a user reports a bug themselves. Business data is not transferred automatically.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 ACCESS CONTROL TO PREMISES AND FACILITIES WHERE DATA IS PROCESSED

a) Access to the contractor's premises used to carry out the order is restricted to those persons required to carry out the order.

b) The entrances to the contractor's premises where personal data is processed are secured with security or magnetic card locks to prevent unauthorised access.

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

d) Doors, gates and windows of the contractor's premises where personal data is processed are kept securely locked outside operating 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 unauthorised persons find it considerably more difficult to gain access, for example through burglar-resistant doors, gates, windows and locks and/or the use of a burglar alarm system, as well as the security measures of security class SG1 described in VdS 2333.

e) Servers used by the contractor to carry out the order are housed in a separately secured server room or data centre, which are separately secured against unauthorised access by an access control system in accordance with class B of VdS 2367. These rooms are burglar-resistant and designed in accordance with at least the requirements of security class SG1 of VdS 2333. Access to these premises is restricted to maintenance and repair personnel and other specifically required roles and persons.

4.2 ACCESS CONTROL

a) The information processing systems (client and server systems) used by the processor to carry out 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 contract shall only be assigned to persons commissioned to perform the contract and only to the extent necessary for the respective task.

c) Each granting of access authorisation is documented for the duration of the order.

d) All accesses and identifiers ("accounts") are assigned exclusively on a personal basis. The use of accounts by several persons (group accounts) is strictly prohibited.

e) Identification and authentication information shall be used exclusively for personal purposes; any password contained in such information shall be assigned as an initial password and shall be changed immediately after receipt by the authorised person in accordance with the provisions set out in this Annex to a password known only to the authorised person; no disclosure shall be made. If unauthorised persons gain knowledge of access data, the processor shall notify the controller immediately.

f) Passwords shall be chosen with sufficient complexity and quality. Sufficient complexity and quality means a minimum length of ten (10) characters using three of the following four categories (upper and lower case letters, numbers and special characters), no use of generic terms or proper names, and the invalidity of at least the last three (3) passwords used.

g) The processor shall keep authentication data (in particular passwords and cryptographic keys) strictly confidential from unauthorised persons, shall not store them in plain text and shall use them exclusively with encryption in accordance with this Annex or as an irreversible cryptographic checksum (in particular when storing and transmitting them in the network).

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

i) Every instance of hardware being issued to the contractor's employees is documented for the duration of the contract.

4.3 ACCESS CONTROL

a) If personal data is stored on the data processor's information processing systems for the purpose of executing the contract, a graded and appropriately granular rights system shall be set up and technically implemented for all access to personal data. This ensures that access rights are designed in such a way that only those employees involved in the provision of services are

granted access to personal data to the extent necessary for the performance of their specific tasks. The granting of administrator rights is limited to the absolutely necessary number of employees of the data processor.

b) All processed data is transmitted in encrypted form. All personal data is stored in encrypted form in our database systems. All access is also via encrypted data channels.

c) If personal data is stored on the data 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 context of order processing (laptops, telephones, etc.) are equipped with automatic screen locking in case of inactivity.

e) A clean desk policy applies in the contractor's premises; desks and other surfaces must be kept free of any documents.

4.4 INPUT CONTROL

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

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

c) The granting of rights to enter, change and delete data in the server systems used is based on an authorisation concept.

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

e) Before installing new programmes and updates on the server systems used, their integrity is ensured by means of functional tests.

4.5 ORDER CONTROL

a) The persons employed by the processor to carry out the order are comprehensively trained in the general principles and specific requirements of data protection, including data security, resulting from these GTC before they are deployed by the processor to carry out the order and then on a regular basis.

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 carry out the order shall be obliged to maintain the confidentiality and protection of personal data. This obligation extends to telecommunications secrecy and the associated principles and requirements for the confidentiality of telecommunications, if this is necessary in accordance with the specific order, in particular if the order includes access to traffic data.

c) Contracts with subcontractors shall be concluded exclusively in writing, after conclusion of a data processing agreement and thorough examination of the technical and organisational measures established by the subcontractor.

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

e) Upon termination of the cooperation with subcontractors, they are instructed to delete all processed personal data in accordance with the regulations.

4.6 SEPARATE PROCESSING OF DATA/SEPARATION CONTROL

a) If personal data is stored on the data processor's information processing systems, the personal data is completely separated from the personal data of other clients, thereby ensuring that personal data can be identified and deleted at any time, e.g. by storing the personal data in a separate client, in a separate partition or under a unique identifier that can be accessed separately.

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

4.7 TRANSFER CONTROL

a) Personal data may not be copied (in particular stored on external data carriers), passed on and/or deleted without authorisation.

b) Data carriers and all documents containing personal data (including any backup copies of personal data and copies of original documents) shall be stored in properly locked data security cabinets used exclusively for the execution of the order, if and as long as they are not being processed in accordance with this appendix.

c) Original documents containing personal data shall be handed over by the persons responsible for managing the process to the persons employed to perform the service and shall be taken back from them after completion of the work.

d) Persons employed in the execution of the order shall only be permitted to make handwritten notes to the extent necessary for the performance of the service and on specially marked work materials (e.g. paginated or coloured paper).

e) Original documents issued in accordance with this appendix or handwritten notes made in accordance with this appendix shall be protected against unauthorised access, even if the workplace is left for only a short time ("clean desk policy").

f) The persons employed by the processor in the execution of the order shall use client systems that are sufficiently secure. All client systems are equipped with firewalls and virus protection and are regularly checked for compliance with current security standards.

g) Personal data shall not be stored on server systems with non-volatile memory used by the processor to perform the contract, e.g. network printers or scanners, beyond the scope immediately necessary for the performance of the contract. If third parties are responsible for the maintenance of such systems, section 5.3 of this appendix shall apply accordingly.

h) WLAN access points provided on the client's premises for network access are encrypted.

i) If, in accordance with the contract, the processor is obliged to delete personal data, the processor shall

   i. delete all electronic data carriers containing personal data that can be deleted (in particular hard drives, USB sticks, floppy disks, tapes) in a manner that complies with data protection regulations and cannot be restored;

   ii. ensure the permanent 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 clause (including all misprints, memory cards, USB sticks, etc. containing personal data) etc.) containing personal data using a commercially available document shredder in accordance with security level 3 as specified in DIN standard 32757 or an at least equivalent procedure, whereby defective magnetic data carriers that cannot be mechanically destroyed as specified above (e.g. defective hard drives) must be deleted using an approved deletion device in accordance with DIN 33858;

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

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

a) Server systems used by the processor to carry out the order are protected by firewalls, which secure these server systems against access that is not necessary for operation.

b) All software used by the contractor to perform the contract is kept up to date and security-related updates (in particular updates, patches, fixes) are installed immediately after they have been made generally available by the software manufacturer and tested by the processor using state-of-the-art procedures. In the case of updates classified as "critical" or similar, the period specified in sentence 1 shall not exceed two (2) days.

c) Original documents containing personal data and personal data lawfully stored by the processor on information processing systems shall be 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 by the contractor shall be treated in the same way as original data, in particular protected against unauthorised access.

e) All server systems used are equipped with fire and smoke detection systems, fire extinguishing systems, air-conditioned server rooms, surge protection measures, video surveillance and alarm systems in case of unauthorised access to the server room.

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

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

h) Data storage is separate 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 results are 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 revocation.

4.10 ORGANISATIONAL CONTROL

a) An external data protection officer is appointed by the contractor.

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

c) All employees of the contractor will be trained at least once a year in data protection issues and existing data protection concepts. Training materials are available in written form and as training videos.

d) Internal guidelines and work instructions apply to the contractor's employees regarding

   a. handling personal data in the home office/mobile office,

   b. Use of company internet access and company email accounts,

   c. Use of private devices for company activities (bring your own device).

e) All employees of the contractor are bound in writing to maintain confidentiality in accordance with data protection laws.

4.11 REGULAR REVIEW AND EFFECTIVENESS MONITORING

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

b) If the review reveals that technological standards or organisational processes have changed and that such changes require adjustments to the measures listed here, the necessary adjustments shall be implemented without delay. In doing so, the principle of appropriateness shall be observed.

c) Changes will also be made on an ad hoc basis if this is necessary for security reasons.

d) The review and any resulting changes will be documented and filed.