DATA PROCESSING AGREEMENT (“DPA”)

FOLLOWING ART. 28 GDPR

between

Users of the web application awork

– in the following called “Principal” –

and the contract processor

awork GmbH

Großer Burstah 36/38

20457 Hamburg

– in the following called “Contractor” –

– in the following together called the “Parties” –

PREAMBLE

For this data processing agreement, the terms and definitions of the Provision (EU) 2016/679 (in the following "GDPR"), in particular Art. 4 GDPR, apply.

1 OBJECT

1.1 The objective of this data processing agreement is the establishment of the data protection framework for the contractual relations between the parties.

1.2 The description of the respective contract with the information about the object of the contract, scope, type and purpose of the data processing, the type of personal data as well as categories of the persons affected are found in the Appendix under Figure 1.

2 LOCATION OF THE DATA PROCESSING

2.1 The contractually agreed-upon processing takes place in the area of the Federal Republic of Germany, in a member state of the European Union, or in another contractual state of the agreement via the European economic space ("Safe states"), insofar as nothing else arises from the Appendix.

2.2 The Contractor may only process or have processed Principal data by agencies outside the safe states ("third country") if and insofar as (i) for the affected third country an appropriate level of data protection is established on the basis of a valid decision of the European Commission or (ii) the processing is done on the basis and according to the respectively valid EU standard contractual clauses ("SCC"), which must be presented to the Principal and agreed upon in writing with the established position in the third country ("data importer"). Insofar as the data importer and the Contractor are not identical, the Contractor must accede to this SCC. The determinations established in this agreement remain undisturbed.

3 TERM

3.1 This contract is concluded for an undetermined time and can be terminated by either party with a deadline of three months. Insofar as, at the time of the termination a primary contract or several primary contracts, in which the Contractor processes personal data of the Principal, are in force, the determinations of this contract are valid until the regular ending of the main contract/the main contracts.

3.2 The Principal can terminate this contract without the upholding of a deadline, if there is a serious infringement of the Contractor against the data protection specifications or the determinations of this contract. In particular, the non-compliance of the obligations agreed upon in this contract and derived from Art. 28 GDPR presents a serious infringement.

4 DIRECTIVE

4.1 The Contractor processes the personal data only in the framework of the directives given by the Principal. This does not apply insofar as the Contractor is obligated to processing through the law of the EU or the member states to which the Contractor is subject. In this case, the Contractor communicates these legal requirements before the processing, unless the communication is prohibited because of an important public interest through the applicable law.

4.2 In case directives change, offset, or supplement the establishments made under Figure 1 of the Appendix of this contact, they are only permitted if a corresponding new agreement is made in writing.

4.3 Independent of the form of the granting, the Contractor as well as the Principal will document each directive of the Principal in text form. The directives are for the length of this contract and subsequently must still be upheld for three years.

4.4 The Contractor will immediately point out to the Principal when a directive granted by the Principal violates legal specifications. In such a case, the Contractor is entitled according to legal prior notice toward the Principal to suspend the execution of the directive until the Principal has changed the directive or has confirmed this. Insofar as the Contractor can present that a processing according to the instruction of the Principal can lead to a liability of the Contractor following Art. 82 GDPR, the Contractor remains free to suspend the further processing until there is a clarification of the liability between the parties.

4.5 Directives may only be granted by persons who because of their executive position or their special function represent the Principal in this respect (e.g. data protection officer, Chief Security Officer, etc.).

4.6 The Contractor establishes a recipient of instructions in the Appendix of this contract. With a change or a long-term hindrance of the contact partner, the follower or representative of the contractual partner must be informed immediately and in written or electronic form.

5 SUPPORT OBLIGATIONS OF THE CONTRACTOR

5.1 In light of the type of the processing, the Contractor will take suitable technical and organizational measures to support the Principal in his obligation to answer applications of the persons affected following Art. 12 to 22 GDPR.

5.2 With consideration of the type of the processing and the information available to it, the Contractor will support the responsible party in the upholding of its obligations following Art. 32 to 36 GDPR. In detail with the security of the processing, in messages about injuries to the supervisory authority, the notification of affected persons in an injury, data protection impact assessment and in consultation with the responsible supervisory authority.

5.3 Insofar as an affected person or a data protection officer turns directly to the Contractor in connection with the personal data processed under this agreement, the Contractor will inform the Principal about this immediately and will coordinate the further steps with him.

6 AUDITING RIGHTS OF THE PRINCIPAL

6.1 The Contractor will make available to the Principal upon its request all necessary information on the proof of the regulated obligations in this contract and in Art. 28 GDPR. In particular, the Contractor will grant to the Principal information about the stored data and the data processing program.

6.2 The Principal or third parties commissioned by is – fundamentally after an agreement on deadline of at least 30 days in advance – entitled to check the upholding of the obligations from this contract and from Art. 28 GDPR and to carry out inspections on site about the Contractor. The Contractor will make this possible and will contribute to it. Groundless inspections are limited to a maximum of one inspection per year.

6.3 The Contractor must deliver to the Principal upon request suitable proof about the upholding of the obligations in accordance with Art. 28 Par. 1 and Par. 4 GDPR. This proof can be rendered through the provision of documents and certificates that display the approved rules of conduct in the sense of Art. 40 GDPR or approved certification procedures in the sense 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 of this agreement under Figure 3.

8 CONFIDENTIALITY

8.1 The Contractor confirms that the data protection provisions of the GDPR applicable for the data processing are known to it. It will maintain data secrecy during the processing of the personal data of the Principal as well as its confidentiality. This obligation continues even after the ending of this contractual relationship.

8.2 The Contractor ensures that it will familiarize itself with engaged employees in the carrying out of the work with the appropriate determinations of the data protection. It obligates these employees to the upkeep of confidentiality through written agreement for the time of the activity and even after the ending of this employment relationship, insofar as no appropriate legal obligation to secrecy exists. The Contractor will oversee the upholding of the data protection regulations in its company.

8.3 The Contractor may deliver to third parties or to those affected only with prior written consent, or agreement in an electronic format, by the Principal.

9 TECHNICAL AND ORGANIZATIONAL MEASURES

9.1 The Contractor will carry out suitable technical and organizational measures in such a way that the processing takes place in agreement with the requirements of the GDPR and the protection of the rights of affected persons is ensured. It will organize its internal organization in such a way that it satisfies the particular requirements of data protection and an appropriate protection level is achieved. In particular, the Contractor will ensure the proper security of the processing with consideration of the respective state of technology, in particular the confidentiality (including pseudonymization and encryption), availability, integrity, and capacity of the systems used for the data processing and services.

9.2 The technical and organizational measures in the Appendix are established as binding.

9.3 The technical and organizational measures can be adjusted in the course of the contractual relationship of the technical advancement. Thus, the adjusted measures must correspond at least to the security level of the measures agreed on in the Appendix. Substantial changes must be agreed upon in written form or in an electronic format.

10 INFORMATION OBLIGATION OF THE CONTRACTOR AND INJURY OF THE PROTECTION OF PERSONAL DATA

10.1 The Contractor will instruct the Principal immediately about any injuries or suspected injuries against this agreement or provisions that relate to the protection of personal data.

10.2 The Contractor will support the Principal in the investigation, damage limitation, and removal of the injuries.

10.3 Should the personal data agreed upon under this agreement be endangered by the Contractor through seizure or confiscation, through an insolvency procedure or a settlement procedure, or through other events or measures by third parties, the Contractor must immediately inform the Principal about this. The Contractor will immediately inform all relevant positions in connection with this that the control of the data lies with the Principal.

10.4 Insofar as audits of the data protection officers are carried out, the Contractor is obligated to make known to the Principal the result, insofar as it affects the processing of personal data under this contract. The

Contractor will immediately remedy the damages established in the audit report and will inform the Principal about them.

11 SUBCONTRACTORS

11.1 The Principal authorizes the Contractor to incorporate subcontractors into the data processing. This does not require a special prior agreement by the Principal. The Contractor will inform the Principal about each intended change in relation to the enlistment or the replacement of a subcontractor at least 6 weeks before the planned change.

11.2 The Contractor must ensure in accordance with the contract that the regulations agreed upon in this agreement also apply to subcontractors. The agreement of the Contractor with the subcontractor must be concluded in writing or in electronic format.

11.3 A commissioning of subcontractors in third-party states takes place only if the special requirements of Art. 44 ff. GDPR are fulfilled.

11.4 The Principal hereby in addition explicitly grants its agreement for the commissioning of the subcontractors listed in the Appendix.

11.5 The Contractor will ensure that the Principal has toward the subcontractor the same rights of instruction and control rights as toward the Contractor in line with this agreement. If a subcontractor does not fulfill its data protection obligations, the Contractor is liable toward the Principal for upholding the obligations of that subcontractor.

11.6 At the demand of the Principal, the Contractor must prove the conclusion of the agreements closed with the subcontractor toward the Principal. The proof must be made in text form. If the Principal raises an objection against the intended change of a subcontractor relationship before its entry into force (within 6 weeks according to 11.1 of this agreement), the Contractor is entitled to terminate the agreement as well as the main agreement in extraordinary fashion.

12 DELETION AND RETURN OF PERSONAL DATA

12.1 After the conclusion of the processing services agreed upon in the main agreement, the Contractor is obligated to delete all personal data that it has received during the course of the data processing within 35 days. This includes in particular the results of the data processing, provided documents and provided data carriers and copies of the personal data. There is no obligation to delete insofar as the Contractor is legally obligated to further store the data according to the law of the EU or the member states. If there is a further obligation for storage, the Contractor must limit the processing of personal data and use the data only for the purposes for which there is an obligation to store. The obligations for the security of the processing exist for the time of the storage. The Contractor must delete the data within 35 days, as soon as the obligation for storage is dropped. Notice: A deletion within fewer than 35 days is not technically possible because of the established back-up concept of the databases used.

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

12.3 The processes must be recorded with the information about the date.

13 LIABILITY

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

13.2 In the internal relationship, the Contractor is only liable for faults toward the Principal that lie within its sphere. The liability regulations of the main agreement remain unaffected in the internal relationship.

14 FINAL PROVISIONS

14.1 The plea for the right of retention following § 273 BGB is excluded with regard for the data processed for the Principal.

14.2 The Appendix, or, in the case of several concluded agreements, the Appendices to this contract are a substantial component of the same.

14.3 For changes or supplementary agreements, the written form or an electronic format is necessary. This applies also to changes of this form requirement.

14.4 Insofar as between the parties agreements on data processing already exist due to the services established in this agreement or taken into account, these agreements will be canceled with the coming into force of this agreement and this agreement will finally regulate the rights and obligations of the parties existing in this respect.

14.5 The parties agree that this agreement should be signed with an electronic signature and alternatively can be drawn up in written form. It can be signed effectively with an electronic signature in such a way that the parties exchange the copies respectively signed by them in electronic form as a .pdf. A signature can likewise be made through the digital online registration process of the Contractor. The Principal guarantees that the person signing or concluding the online registration process (representative) has all powers and rights of representation necessary for the conclusion of this agreement. The Principal will have all explanations of the representative paid off. Changes to this agreement, including its appendices, likewise underlie the form requirements regulated in this figure.

14.6 If a determination in this agreement proves to be ineffective, this does not affect the effectiveness of the remaining provisions of the agreement.

14.7 This agreement is subject to German law. The place of jurisdiction for disputes from this agreement corresponds to the regulation of the main agreement.

APPENDIX ON THE DATA PROCESSING AGREEMENT

1 OBJECT OF THE ORDER

1.1 OBJECT OF THE ORDER:

The processor is the manufacturer and provider of company software for the processing of all project-related commercial processes. Among these are the sale, the advising, implementation as well as integration, hosting, and support of the solutions. The levying, processing, and use of data is done for the exercise of the above-named purposes.

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

The processing of personal data is done for the purpose of the provision of the Software-as-a-Service use of awork, with whose help the work, team and project organization of the Principal takes place. This means in particular

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

For this purpose, personal data is recorded, stored, read, organized and ordered, displayed in user interfaces, as well as deleted.

1.3 CIRCLE OF THOSE CONCERNED AND TYPE OF DATA:

The following groups of persons will have their personal data levied, processed, and used, insofar as this is necessary for the fulfillment of the named purpose:

- **Internal and external employees (e.g. freelancers) & temporary help of the Principal:**
  - Professional contact and (work) organization data for the administration of users: Name, First name, Sex, Email, Phone number, Photo
  - Data on professional relationships: Professional designation, log-file information, IP address, work time, absence times, activities
- **Interested parties, customers and other business partners of the Principal**
  - Professional contact and (work) organization data: Name, First name, Email, Phone number

2 AUTHORIZED PERSONS

2.1 AUTHORIZED PERSONS OF THE PRINCIPAL:

Directives may only be granted by persons who because of their executive position or their special function represent the Principal in this respect (e.g. data protection officer, Chief Security Officer, etc.).

2.2 INSTRUCTION RECIPIENTS OF THE CONTRACTOR ARE:

Name: Bauche, Lucas

Function: Manager

Communication channel for instructions: privacy@awork.io

Representative:

Name: Czernig, Nils and Hagenau, Tobias

Function: Manager

Communication channel for instructions: privacy@awork.io

3 DATA PROTECTION OFFICER

The data protection officer of the Contractor is:

PROLIANCE GmbH

www.datenschutzexperte.de

Leopoldstr. 21

80802 Munich

datenschutzbeauftragter@datenschutzexperte.de

4 SUBCONTRACTORS

The following belong to the circle of approved subcontractors at the conclusion of this agreement:

4.1 HOSTING

The complete hosting of the awork application is done in European data centers. For this, the following data center operator is used:

Microsoft Ireland Operations Ltd, South County Business Park, Dublin, Ireland

- Storage of the application data in persistent databases
- Operation of the application and primary data processing
- Contractual basis: Data Processing Agreement from 09/12/2021
- Guarantees: EU Standard contractual clauses, ISO 27001 cert. Server location guaranteed in the EU

4.2 OTHER DATA PROCESSORS

HQLabs GmbH, Colonnaden 41, 20354 Hamburg, Germany

- HQLabs from Hamburg provides support for awork users. When an awork user opens a support case, that user's name and email are transferred to HQLabs in order to answer queries.
- Contractual basis: Data Processing Agreement from 03/28/2022

Twilio Ireland Limited, 25-28 North Wall Quay, Dublin 1, Ireland

- Segment by Twilio is a tool to manage application data. It is used to transfer relevant usage-data to intercom (see above) in order to handle support cases.
- Contractual basis: Data Processing Agreement from 04/04/2022
- Guarantees: EU standard contractual clauses, Binding Corporate Rules

Intercom Inc., 55 2nd Street 4th Floor San Francisco, CA 94105, USA

- Intercom is a communications tool. It is used to give users of the software the opportunity to chat with the support and the sales team and allows users to send automated messages (e.g. with instructions).
- Contractual basis: Data Processing Agreement from 03/23/2022
- Guarantees: EU standard contractual clauses

5 TECHNICAL AND ORGANIZATIONAL MEASURES

5.1 ACCESS CONTROL TO SPACES AND FACILITIES IN WHICH DATA IS PROCESSED

a) Access to the spaces of the Contractor that are used for the carrying out of the order is limited to the persons necessary for the carrying out of the order.

b) The entrances to the spaces of the Contractor in which personal data is processed are secured against access by those not authorized with safety and magnetic card locks.

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

d) Doors, gates, and windows of the spaces of the Contractor in which personal data is processed are firmly closed outside of operating times; doors, gates and windows in cellars and on the ground floor as well as all further easy-to-reach accesses to these spaces are designed in such a way that these are accessible to those not authorized only in a very difficult fashion, such as through burglar-resistant doors, gates, windows, and locks, and/or the use of a burglar alarm system, as well as the safety measures of safety class SG1 described in the VdS 2333.

e) The servers used to carry out the order by the Contractor are housed in a separately secured server room or data center, which are specially secured through an access control system in accordance with Class B following VdS 2367 against access by unauthorized persons. These spaces are protected against break-in and executed at least in accordance with the provisions of safety class SG1 following VdS 2333. Access to these spaces is limited to maintenance and repair as well as to the overall concretely necessary roles and persons.

5.2 ACCESS MONITORING

a) The information-processing systems used for the carrying out of the order from the order processor (client and server systems) are protected by authentication and authorization systems.

b) Identification and authentication information (in particular in the form of user names and passwords) that are connected with the access authorization on the information-processing systems used for the carrying out of the order are only assigned to the persons commissioned with the carrying out of the order and merely in the scope necessary for the respective task.

c) Each awarding of access authorizations is documented for the length of the order.

d) All accesses and identifications ("Accounts") are awarded exclusively person-specific. The use of accounts by several persons (group accounts) is stopped fundamentally.

e) Identification and authentication information are used exclusively personally; a password contained in such information is awarded as an initial password and is immediately converted after the receipt by the authorized person corresponding to the determinations established in this Appendix to a password known only to the authorized person; any disclosure is stopped. If unauthorized persons receive access data, the order processor will immediately show this to the responsible party.

f) The choice of the passwords is done with sufficient complexity and quality. Sufficient complexity and quality means at least a length of ten (10) characters in the use of three of the following 4 categories (upper- and lowercase letters, figures and special characters), no use of generic terms or of personal names as well as the inadmissibility of at least the last three (3) passwords used.

g) The order processor will keep authentication data (in particular passwords and cryptographic keys) strongly secret toward unauthorized persons, preserve these not in plain text, and use this exclusively using an encryption corresponding to this appendix or as an irreversible cryptographic checksum (in particular in the storage and transfer in the network).

h) For the encryption, the AES algorithm with 256 bits and for passwords hashes of the HMAC algorithm with 512 bits are used.

i) Each surrender of hardware to the employee of the Contractor is documented for the length of the order.

5.3 DATA ACCESS MONITORING

a) Insofar as personal data is stored for the carrying out of the contract on information-processing systems of the data processor, for all access to personal data, a graduated and suitably granular system of rights is established and technically implemented. It is thereby ensured that the access rights are designed so that they allow only the employees engaged for the performance of the service access to the personal data necessary for the fulfilling of concrete tasks in the necessary scope. Thus, the awarding of administrator rights is limited to the absolutely necessary extent of employees of the order processor.

b) All processed data is transferred encrypted. All personal data is filed in our database systems in encrypted format. Each access takes place likewise via encrypted data channels.

c) Insofar as personal data is stored on information-processing systems of the order processor, all access to personal data (including the reading, changing, and deleting access) is logged according to user, date, time and the respectively affected personal data for a length of at least 90 days.

d) All end devices used in the framework of the order processing (laptops, phones, etc.) are provided with automatic screen lock in case of inactivity.

e) In the spaces of the Contractor, there is a clean-desk policy; desks and other areas must be left free of any documents.

5.4 INPUT CONTROL

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

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

c) The awarding of rights to input, change, and delete data in the server systems used is done on the basis of an authorization concept.

d) Files and documents are stored in document management systems, which automatically record the inputs and changes with date and user recognition.

e) Before the installation of new programs and updates on the server systems used, their integrity is ensured through function tests.

5.5 ORDER CONTROL

a) Following the general principles as well as the specific requirements on data protection arising from this agreement, including data security, the persons engaged by the order processor for the carrying out of the order are trained before use by the order processor for the carrying out of the order and then regularly in extensive fashion.

b) At the end and on the basis of the a) training processes established in this section, the persons engaged by the order processor for the carrying out of the order are obligated to confidentiality and to the protection of personal data. This obligation extends to the secrecy of telecommunications and the associated principles and requirements to the confidentiality of telecommunications, if this is necessary according to the concrete order, in particular if the order comprehends access to traffic data.

c) The awarding of orders to subcontractors is done exclusively in writing, after the conclusion of a data processing contract and extensive review of the technical and organizational measures established by the subcontractor.

d) A central directory of all concluded data processing contracts of the commissioned subcontractor is managed.

e) After the ending of the collaboration with subcontractors, these are instructed to delete all processed personal data in an orderly fashion.

5.6 SEPARATE PROCESSING OF DATA/SEPARATION CONTROL

a) Insofar as personal data is stored on information-processing systems of the order processor, a complete separation of the personal data from the personal data of other principals is realized and thus the constant and complete ability to identify and delete personal data is ensured, e.g. through the storage of personal data in one of their own clients, in their own partition, or retrievable separately under a unique identifier.

b) A corresponding separation is also realized for personal data if it is stored for special purposes.

5.7 TRANSFER CONTROL

a) Personal data cannot be copied unauthorized (in particular stored on external data carriers), forwarded, and/or deleted.

b) Data carriers as well as all documents, insofar as they contain personal data (including all possibly available safety copies of personal data and copies of original documents) are stored in orderly and locked fashion and in data protection cabinets used exclusively for the carrying out of the order, if and so long as they are not in processing according to this Appendix.

c) Original documents that contain personal data must be issued by the persons responsible for the process to the persons engaged for the performance of the service and again received by these after the conclusion of the work.

d) The persons engaged in the carrying out of the order are permitted the preparation of hand-written records only in the scope necessary for the performance of the service and in specially marked work materials (e.g. paginated or colored paper).

e) Original documents issued according to this Appendix or hand-written records created according to this Appendix are, even with a short-term departure from the workplace, protected against unauthorized access ("Clean Desk Policy").

f) The persons engaged in the carrying out of the order by the order processor use client systems that are sufficiently secured. All client systems are provided with a firewall and virus protection and are regularly checked for common security standards.

g) In the carrying out of the order by server systems used by the order processor with non-volatile storage, e.g. network printers or scanners, personal data is not stored above the scope needed immediately for the carrying out of the contract. Insofar as third parties are entrusted with the maintenance of such systems, Figure 5.3 of this Appendix applies.

h) In the spaces of the Principal, Wi-Fi access provided for network access is encrypted.

i) If according to the order for the order processor there is an obligation to delete personal data, the order processor

i. will carry out the data protection, non-reproducible deletion of all deletable electronic data carriers that contain person data (in particular hard drives, USB sticks, diskettes, tapes);

ii. will realize the sustainable and irreversible removal of personal data from database or file systems as well as all other deletable storage media;

iii. destroys all paper documents containing personal data and other deletable data carriers not in line with (i) or (ii) of this figure (including all misprints, storage cards, USB sticks, etc. containing personal data) with a customary document destroyer in accordance with security level 3 in accordance with DIN Norm 32757 or an at least equivalent procedure, whereby defective magnetic data carriers that cannot be destroyed mechanically as given above (e.g. defective hard drives) must be deleted using a permitted deletion device in accordance with DIN 33858;

iv. record the deletion for the length of the order.

5.8 AVAILABILITY AND CAPACITY (ART. 32 PAR. 1 LET. B GDPR)

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

b) All software possibly used by the Contractor for the carrying out of the order is kept updated and security-relevant updates (in particular updates, patches, fixes) are immediately brought in, after these are made available by the manufacturer of the software and tested by the order processor in the course of a procedure corresponding to the state of the technology. For updates qualified as "critical" or the like, the deadline in accordance with Sentence 1 amounts to at most two (2) days.

c) Original documents that contain personal data, as well as personal data stored by the order processor legally on information-processing systems, are protected by technical and organizational measures against loss through chance, negligent, or intentional deletion or change.

d) Backup files of personal data stored legally on information-processing systems are treated like original data according to the same measures, and in particular are secured against unauthorized access.

e) All server systems used have fire and smoke alarm systems, fire extinguishing systems, climatized server rooms, protective measures against overvoltage, video oversight as well as alarm message systems against unauthorized access to the server room.

f) All storage systems have redundant storage media (e.g. RAID systems, reflections or the same).

g) The Contractor has a backup and recovery concept, which makes possible the restoration of backups from the last 30 days.

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

i) The storage of data and backups is done in at least two separate fire protection zones.

j) The data restoration is tested regularly and the test result is recorded.

5.9 DATA PROTECTION-FRIENDLY DEFAULT SETTINGS, PRIVACY BY DEFAULT

a) Personal data is levied no more than is necessary for its respective purpose.

b) Through suitable technical measures (independent initiation and confirmation of the deletion procedure), the simple exercise of the right of revocation of the affected persons is ensured.

5.10 ORGANIZATION CONTROL

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

b) The commissioned data protection officer is supported in his work by an internal employee (“Lead-function data protection”).

c) All employees of the Contractor are trained in data protection questions and present data protection concepts at least once per year. Training materials are available in writing and as training videos.

d) For employees of the Contractor, there apply internal guidelines and work instructions on

   i. handling of personal data in a home office / mobile office,

   ii. use of the operational Internet access and the operational email accounts,

   iii. use of private devices for operational activities (Bring your own device).

e) All employees of the Contractor are obligated in writing to confidentiality as regards data protection.

5.11 REGULAR REVIEW AND EFFICIENCY CONTROL

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

b) In case, through review, it is established that technological standards or organizational processes have changed and such changes make necessary an adjustment of the measures listed here, the thus necessary adjustment will be implemented immediately. Thus, the fundamental of adequacy is observed.

c) In addition, changes are carried out on an ad hoc basis, insofar as this is necessary for reasons of security.

d) The review as well as the resulting changes are documented and filed.