Data Processing Agreement / Commissioned Data Processing Agreement (CDPA)

HORNETSECURITY

Between

The Customer

(hereinafter "Customer")

and

Hornetsecurity GmbH
Am Listholze 78
30177 Hannover
Germany

(hereinafter "**Hornetsecurity**")

as a commissioned subcontractor by

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Germany

(hereinafter "**Contractor**")

has been agreed to as follows:

1. Object and characteristics of commissioned data processing

This Commissioned Data Processing Agreement governs the handling of personal data by Hornetsecurity within the scope of the contract concluded between the Customer and the Contractor. This Commissioned Data Processing Agreement shall take precedence, with regard to the handling of personal data, over the Service Contract and Hornetsecurity's existing confidentiality or legal obligations to retain data. Hornetsecurity processes this personal data for the Customer within the meaning of Articles 4 No. 2 and Art. 28 of the General Data Protection Regulation (GDPR).

Object, scope, type and purpose of the data processing are determined by the Service Contract. The type of processing (Art. 4 (2) GDPR) of personal data, the categories of data subjects as well as authorized persons and recipients are regulated in **Annex 1** of this CDPA. In the event of a change or if the contact persons are unable to fulfill their obligations for a period of time, the contractual partners, or their successors or representatives, must be informed immediately, in writing or electronically. The term of this CDPA corresponds to that of the Service Contract. The Customer may terminate this contract at any time without notice if Hornetsecurity commits a serious breach of data protection regulations or the provisions of this contract, if Hornetsecurity is unable or unwilling to comply with an instruction given by the Customer, or if Hornetsecurity refuses to allow the Customer control rights in breach of this Agreement. Non-compliance with the obligations agreed in this contract and derived from Article 28 GDPR constitutes a serious violation.

The term of this CDPA corresponds to that of the Service Contract. The Customer may terminate this contract at any time without notice if there is a serious breach by Hornetsecurity of data protection regulations or the provisions of this contract and if the Customer therefore cannot be expected to adhere to the contract.

Amendments to this Agreement must be regulated centrally in **Annex 4** and shall only take effect if they are listed therein. In all other respects, the unchanged specimen contract shall be considered to have been agreed, as shown in the footer. The regulations in **Annex 4** take precedence over those of the main text of the agreement as well as those of **Annexes 1 - 3** in the event of overlaps or collisions.

The processing of the data by Hornetsecurity shall take place exclusively in a member state of the European Union or in another state that is party to the Agreement on the European Economic Area. Any transmission or other relocation of the data to a third country requires the prior consent from the Customer and may only take place if the special legal requirements of Art. 44 ff. GDPR are fulfilled (e.g. determination of adequacy of the commission, standard data protection clauses, approved codes of conduct).

2. Rights and obligations of the Customer

2.1. Responsibility for data processing

The Customer shall remain exclusively authorized to determine the processing of the data.

The Customer bears responsible against Hornetsecurity for the processing and shall be responsible against third parties for compliance with the provisions of the data protection laws.

It shall be the Customer's responsibility to assess the legitimacy of the order data processing and the order with regard to data protection law. If the Customer is of the opinion that the processing by Hornetsecurity violates the Customer's obligations, the Customer shall inform Hornetsecurity of this and ensure a legally compliant data processing through appropriate instruction.

2.2. Notifications

In the event of a direct request for information, notification, warning or instruction from the supervisory authority to Hornetsecurity pursuant to Art. 58 GDPR, the Customer shall assist Hornetsecurity, thus ensuring that the official request can be complied with in accordance with this CDPA.

3. Obligations of Hornetsecurity

3.1. Obligation to instructions

3.1.1. Hornetsecurity shall process the personal data exclusively within the framework of the concluded agreements and according to the Customer's instructions. The Customer has a comprehensive right to instruction regarding the type, scope and procedure of the data processing, which he can specify through individual instructions; this shall not affect statutory obligations of Hornetsecurity (e.g. concerning investigations by law enforcement or state security authorities); in such a case, Hornetsecurity shall inform the Customer of these legal requirements before processing, provided that the law does not forbid such notification on account of significant public interest (Article 28 (3) (2) (a) GDPR).

3.1.2. The Customer shall convey all orders, partial orders, and instructions in writing or in text form by means of the agreed channels of communication. At a minimum, oral instructions shall be immediately confirmed by the Customer in writing. Both parties shall retain the instructions for their period of validity and for three full calendar years thereafter.

3.1.3. If an instruction or a commissioned data processing violates legal data protection laws, Hornetsecurity shall inform the Customer directly (Art. 28 (3) (3) GDPR). This shall also apply in the event that the Client's instructions deviate from those of a controller.

3.1.4. Changes to the processing object and changes in procedure must be agreed to and documented by both the Customer and the Contractor.

3.1.5. Hornetsecurity shall use the data for no other purpose, and shall not pass the data on to third parties without authorization. Copies and duplicates shall not be made without the Customer's knowledge. This excludes security copies, if they are necessary for the carrying out of contractually arranged data processing, and storage of data which is necessary for compliance with legal retention obligations.

3.1.6. Hornetsecurity may only provide information to third parties or the data subjects after examination and approval by the Customer, unless Hornetsecurity is required to provide such information by law or by a legally binding official or court order. Hornetsecurity shall forward all requests with regard to the data regulated by this CDPA immediately to the Customer, unless Hornetsecurity is legally obligated to their surrender to the Customer without notification. Item 3.6.4 remains unaffected.

3.2. Data secrecy and confidentiality obligation

3.2.1. Hornetsecurity shall ensure that all of its employees with the ability to access the Customer's personal data in a contractual capacity, or the ability to otherwise obtain knowledge of the Customer's data, have been familiarized with the relevant data privacy laws beforehand, and are bound to secrecy in a suitable manner for the time period of their work as well as after the end of the work relationship (Article 28 (3) (2) (b) and Article 29 GDPR).

3.2.2. Hornetsecurity shall ensure that all of its employees who may be involved as other participating persons in the pursue of a profession subject to secrecy within the sense of §203 of the German Criminal Code (StGB) shall be obligated to secrecy in a suitable manner in the event of obtaining private secrets for the duration of their employment as well as after termination of the employment.

3.2.3. Any other third parties who have the ability to access the Customer's personal data through their contracted work are to be obliged to confidentiality accordingly. Hornetsecurity shall undertake suitable measures to ensure that third parties with access to the Customer's data shall not process this data beyond what was arranged by the contracting parties, and that the Customer's instructions with regard to this contract shall also be carried out by said third parties.

3.3. Technical and organizational measures

3.3.1. Hornetsecurity shall monitor the compliance of data privacy laws in Hornetsecurity's operations.

3.3.2. Hornetsecurity undertakes to implement and comply with the technical and organizational measures (TOM) described in **Annex 2** and guarantees that these have been defined taking into account the requirements of Article 32 GDPR and that the protection objectives such as confidentiality, integrity and availability of the systems and services and their resilience with regard to the type, scope, circumstances and purpose of processing are thus taken into account in such a way that the risk is permanently contained by appropriate technical and organizational remedial measures. Hornetsecurity shall also ensure, for the specific processing of the contract, a level of protection appropriate to the risk to the rights and freedoms of the natural data subjects. At the Customer's request, Hornetsecurity shall disclose the detailed circumstances unless, in particular interests of secrecy, Hornetsecurity's protection-worthy overriding interests outweigh the disclosure.

3.3.3. The Customer is obliged to provide in a timely manner to Hornetsecurity, before conclusion of the contract and during its term, all the information necessary to Hornetsecurity with respect to the requirements of Article 32 GDPR. The Customer especially notes that if special categories of personal data are to be processed in accordance with Article 9 GDPR or if special circumstances arise from other reasons, there is an increased likelihood of occurrence or seriousness of risk to the rights and freedoms of the data subject.

3.3.4. The technical and organizational measures shall be subject to technical progress and continued development. In this respect, Hornetsecurity is permitted to implement adequate alternative measures. However, the safety level of the specified measures must not fall short of that specified. Significant changes must be documented. Hornetsecurity must regularly carry out a review, evaluation and evaluation of the effectiveness of the TOM to guarantee the security of processing as appropriate (Article 32 (1) (d) GDPR).

3.3.5. Hornetsecurity can also prove to the Customer the implementation of technical and organizational measures through the submission of current certificates, reports or report extracts from independent bodies (e.g. external or internal audits, data protection officer, IT security department, data protection auditors, quality auditors) or an appropriate certification from an IT security or data protection audit (e.g. in accordance with ISO/IEC 27001:2015).

3.4. Use of subcontractors

3.4.1. Hornetsecurity may only hire subcontractors for the processing of the Customer's data with the Customer's specific or general consent (Article 28 (2) GDPR).

3.4.2. Approved subcontractors are listed in **Annex 3**.

3.4.3. Otherwise, the Customer grants general approval for the hiring of subcontractors by Hornetsecurity with the concluding of this Agreement. Hornetsecurity shall inform the Customer of any planned enlistment, change, or replacement of subcontractors, for which the Customer shall have the opportunity to object to such changes. The Customer's objection must be made promptly, and no later than one month after learning of this information.

3.4.4. Hornetsecurity must also ensure that it carefully selects subcontractors, taking particular account of the suitability of the technical and organizational measures taken by the subcontractor within the meaning of Article 32 GDPR. The contracting of subcontractors in third-party countries may only take place if the special legal preconditions of Article 44 ff. GDPR are fulfilled (e.g. determination of adequacy of the commission, recognized standard data protection clauses, approved codes of conduct).

3.4.5. Hornetsecurity shall contractually ensure that rules are agreed with the subcontractor which correspond to those between the Customer and Hornetsecurity arising from this agreement. Hornetsecurity shall ensure the implementation of these obligations on behalf of the Customer and shall, in particular, if necessary, carry out appropriate inspections and inspections, including on-site inspections at the subcontractor's premises, or have them carried out by third parties commissioned by Hornetsecurity. The Customer has the right to obtain information from Hornetsecurity about the essential content of the contract and the implementation of the data protection obligations in the subcontract relationship, if necessary, through the inspection of the relevant contract documents.

3.4.6. The contract with the subcontractor must be made in writing, which also may be done in electronic format (Article 28 (4) and (9) GDPR). The forwarding of data to the subcontractor is not permitted until the subcontractor has fulfilled the obligations laid down in Articles 29 and 32 (4) GDPR with regard to its activities.

3.4.7. Hornetsecurity must regularly and thoroughly monitor the subcontractor's compliance to these obligations. The results of this monitoring must be documented and made available to the Customer on request. Hornetsecurity shall be liable to the Customer for the subcontractor's compliance with the data protection obligations contractually imposed on it by Hornetsecurity in accordance with Item 3.4.

3.4.8. Services necessary for the performance of services which are part of generally recognized and customary business operations, and whose use is foreseeable for the Customer (e.g.

telecommunication services, cleaning staff, etc.) are not to be understood as subcontractual relationships within the meaning of this provision, even if the knowledge of personal data cannot be excluded in individual cases. Hornetsecurity remains obliged to take appropriate and reasonable measures to guarantee the protection and security of the Customer's personal data.

3.4.9. Hornetsecurity operates its infrastructure in an external data centre. However, it is contractually, technically and organizationally ensured that any access to Hornetsecurity's data by the computer center operator is excluded. The specific computer centre used is listed in **Annex 3**.

3.5. Participation in responding to the rights of data subjects

3.5.1. The Customer is solely responsible for the protection of data subject rights in accordance with Articles 12 - 22 GDPR.

3.5.2. If a data subject contacts Hornetsecurity directly, e.g. for the purpose of the rectification or erasure of his/her data, Hornetsecurity will immediately forward this request to the Customer for a decision. Hornetsecurity shall rectify, erase, or block the contractually processed data only with express instruction from the Customer. This does not apply in the case of a corresponding legal obligation and in the case of Item 3.7.4. Hornetsecurity may only provide information to data subjects or to third parties with the prior consent of the Customer.

3.5.3. Hornetsecurity is obliged to cooperate as part of the fulfillment of information obligations in accordance with Articles 12-14 GDPR if the information is not otherwise available, or already made available, to the Customer.

3.5.4. Hornetsecurity is solely obliged to surrender personal data to the Customer in the format in which Hornetsecurity received said data from the Customer for its processing within the scope of this contract, or processed the data according to the terms of the contract. Both surrender in another structured, common, and machine-readable format as well as surrender directly to the data subject or another person designated by him/her are only owed on the basis of an explicit instruction and with assumption of the additional costs incurred.

3.6. Support with data breaches, impact assessments, objections

3.6.1. Hornetsecurity shall immediately inform the Customer of any discovered violation of the protection of personal data under this CDPA. The notification shall contain a description of the type of breach of the protection of personal data, indicating where possible the categories and approximate number of data subjects, categories, and personal data records concerned. The Customer alone shall assess the risk associated with the infringement. Hornetsecurity shall hereby cooperate by reporting the infringement and providing information.

3.6.2. Hornetsecurity assists the Customer in its obligations to cooperate in a data protection impact assessment if the Customer requires further information in addition to the information to be provided by Hornetsecurity in accordance with this agreement.

3.6.3. Should recommendations of the supervisory authority pursuant to Article 36 (2) GDPR become the basis for processing under this Data Processing Agreement, the Customer must confirm these through express instruction. This also applies in particular to recommendations which Hornetsecurity receives directly from the supervisory authority. Hornetsecurity shall inform the Customer of the recommendations and extensions communicated by the supervisory authority in accordance with Article 36 (2) GDPR.

3.6.4. Hornetsecurity shall inform the Customer of any other objections, inquiries or requests concerning data processing received from supervisory authorities or data subjects, in particular regarding control procedures, investigations or other measures by supervisory authorities, provided that applicable law does not prohibit such a notification due to significant public interest.

3.6.5. Hornetsecurity shall provide the Customer with all necessary information. This also relates in particular to information for the defense against third-party claims or with regard to supervisory authority requirements.

3.7. Surrender and erasure of data

3.7.1. Hornetsecurity is obligated to retain the Customer's data inventory for a period of 30 days after expiration of the contract. The Customer may demand, at any time during the contractual period until the expiry of this time period, the surrender or erasure of the stored data. Hornetsecurity shall have no right to retention.

3.7.2. If the Customer issues Hornetsecurity a binding instruction to erasure, in writing or in a documented electronic format, Hornetsecurity must immediately carry out the data deletion, also before expiry of the retention period, in accordance with Item 3.7.1. The data which Hornetsecurity is legally required to retain shall be the only exception. The Customer shall be provided with confirmation of the data's deletion and/or destruction in writing or in documented electronic format, including the date.

3.7.3. If the Customer has neither requested the data to be surrendered nor requested the deletion of the data by the end of the period pursuant to Item 3.7.1, Hornetsecurity must notify the Customer of the data deletion in writing or in a documented electronic format within 10 days. Hornetsecurity is authorized to delete the Customer's data after that deadline has passed.

3.7.4. Documentation which serves as proof of data processing in accordance with the order and the contract shall be kept by Hornetsecurity beyond the end of the contract, in accordance with the respective retention periods, or may be submitted to the Customer.

3.8. Obligation to cooperate in information and control procedures

3.8.1. The Customer may monitor compliance with the provisions on data protection and data security, as well as the contractual agreements, including the technical and organizational measures in accordance with **Annex 2**, itself or by third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as through monitoring, random checks, and inspections on-site (Article 28 (3) (2) (h) GDPR). Hornetsecurity is obliged to fully cooperate with these measures in a supporting manner.

3.8.2. With regard to the control obligations of the Customer, Hornetsecurity shall ensure to satisfy the Customer that the relevant technical and organizational measures have been observed. Upon request, Hornetsecurity shall provide the Customer with proof of the implementation of the necessary technical and organizational measures. Proof may also be provided by the submission of a current audit certificate, of reports or report extracts from independent bodies (e.g. external or internal auditing bodies, data protection officer, IT security department, data protection or quality auditors) or a appropriate certification through an IT security or data protection audit.

3.8.3. Within the context of Item 3.8.1, Hornetsecurity is solely obliged to accept and cooperate with an annual on-site inspection. Hornetsecurity shall only be obliged to accept and cooperate with further controls, in particular multiple inspections, if reimbursed for the additional costs incurred by them. This does not apply to controls which become necessary due to a security issue or not-insignificant violation of the obligations according to this CDPA.

3.8.4. If a security incident or breach of obligations under this CDAP affects the personal data of several controllers for whom the Client is acting, Hornetsecurity shall nevertheless only be obliged to tolerate one single inspection in this context. In case of doubt, the Customer shall carry these out jointly for all controllers.

3.9. Data protection officer

Hornetsecurity has appointed a data protection officer in accordance with the statutory requirements, as per **Annex 1**. Where no data protection officer is named in **Annex 1**, Hornetsecurity ensures that such an appointment is not legally required. A change of data protection officer shall be immediately reported to the Customer.

4. Liability

4.1. Hornetsecurity shall only be liable to the Customer for culpably caused breaches of obligation in accordance with the corresponding provisions of the Service Agreement.

4.2. Insofar as Hornetsecurity's liability is limited or excluded, the Customer shall indemnify Hornetsecurity against all claims brought against Hornetsecurity by third parties on account of the commissioned data processing.

5. General provisions

5.1. Hornetsecurity shall undertake to immediately inform the Customer about the exclusion of approved rules of conduct according to Article 41 (4) GDPR or the revocation of a certification according to Article 42 (7) GDPR.

5.2. Ancillary agreements must be made in written form or in a documented electronic format.

5.3. Hornetsecurity shall immediately inform the Customer if the Customer’s property or personal data to be processed should be endangered by third-party measures (such as seizure or confiscation), by insolvency or settlement proceedings or by other events.

5.4. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

5.5. For all disputes in connection with this CDPA, Hornetsecurity's registered business is agreed to be the exclusive place of jurisdiction. Hornetsecurity remains entitled to sue the Customer at the Customer's general place of jurisdiction.

Annex 1: Details on Hornetsecurity's data processing, contact partner, data protection officer

Annex 2: Technical and organizational measures (TOM)

Annex 3: Authorized subcontractor(s)

Annex 4: Amendments to the text of the contract

	Hannover, 15.09.2020
Place, Date	Place, Date
Customer	**Contractor**

Annex 1: Details on Hornetsecurity's data processing, contact partner, data protection officer

1.) Type of processing (Art. 4 (2) GDPR)

- Collect
- Record
- Organize
- Sort
- Storage
- Modification or change
- Cull
- Retrieve
- Utilize
- Disclosure through transmission
- Distribution or another form of provision
- Matching or linkage
- Restriction, erasure or destruction
- ...

2.) Type of personal data (corresponding to the definition in Article 4 (1), (13), (14), (15) GDPR):

- Name
- Address
- Other personal master data
- Communication data (e.g. telephone, email)
- Contract master data (contractual relationship, contractual interest)
- History
- Contract billing data and payment data
- Planning and scheduling data
- Location data
- Email and webfilter communication metadata
- ...

3.) Categories of data subjects (corresponding to the definition in Art. 4 (1) GDPR):

- Clients
- Potential clients
- Employees
- Applicants
- Suppliers
- Sales representatives

- Contact partners

4.) Authorized issuers of the Customer's instructions, recipients of instructions on behalf of Hornetsecurity

The client's authorized persons are managed by Hornetsecurity in the central configuration directory (Control Panel) and are to be named by the client at the conclusion of the contract.
Authorized persons of the client are:

[first name, last name, organization unit, telephone, email address]

The recipients of the instructions at Hornetsecurity are all employees of Hornetsecurity who are in contact with the client.

The client usually issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

Communication channels to be used for instruction are
By phone: +49 511 515 464-700
By email: support@hornetsecurity.com
By letter: Hornetsecurity GmbH, Am Listholze 78, D-30177 Hannover, Germany

5.) Contractor's data protection officer:

Jurist Lukas Wagner, LL.M.
HK2 Comtection GmbH
Hausvogteiplatz 11 A
D-10117 Berlin
Germany
privacy@hornetsecurity.com

Annex 2: Technical and organizational measures

Selection according to §32 GDPR
Created: 26.03.2018
Last updated: 06.07.2022

Measures	Description
1. Encryption and pseudonymisation of personal data	
Encryption of data records	Data that does not necessarily have to be in plain text for service provision purposes are rendered unrecognisable using common encryption methods. In particular, mail content (spam filter) and data stored in the cloud (Hornetdrive) are only available in databases in encrypted form. Core database: Encryption of email header and body with AES 128 bit; a different key is used for each customer. Email address is used as a search key and it is not stored pseudonymised or encrypted, as this would cause an unacceptable degradation in service functionality. 365 Total Backup & 365 Total Protection Enterprise Backup: Backup data is encrypted with an individual AES 256 bit key. Hornetdrive: All files stored in Hornetdrive are encrypted with a symmetric AES 256 bit algorithm before being uploaded to the user's terminal equipment.
Pseudonymisation of data records	When displaying the user and usage data of the web filter service, the user names/mail addresses can be replaced at the customer's request by a pseudonym, which will change at regular intervals.
2. Confidentiality and integrity	
2.1 Equipment access control	

Measures	Description
Building security (Data centre)	The property boundary of the operator is marked by structural elements such as fences, gates, posts. Access to the controlled internal area is only possible through doors by ringing a bell. Access to the internal area is controlled by two mechanisms: with an electric door opener at the first door using an intercom to the control room, and with a magnetic card at the second door using a locking system. In the restricted area, the processing systems are protected by their own locking system. The premises are additionally monitored by video surveillance. Alarm plans exist for scenarios such as unauthorized intrusion. For further information, please refer to the TOM of the data centre operator.
Accreditation(Data centre)	The operators have lists of names of accredited persons at their disposal (positive list). Personnel with authorised access includes hardware maintenance personnel, project managers, senior management and IT security officers.Following a check of personal details, access is only permitted with an ID of a data centre operator. The entering and leaving of premises is logged.Visitors must be registered and accompanied by an accredited person.For further information, please refer to the TOM of the data centre operator.
Access logging (Data centre)	Persons entering and leaving of the internal area are recorded by the operator, including name, company affiliation, time stamp (start & end of access). For further information, please refer to the TOM of the data centre operator.
Video surveillance (Data centre)	Additional video surveillance is available for all technical rooms, access routes and perimeter protection. This is available on the data centre premises and it is supported by additional motion sensors. For further information, please refer to the TOM of the data centre operator.

Measures	Description
Alarm system (Data centre)	Access routes and premises are monitored by an alarm system. Processes have been defined to deal with any issues/occurrences of note. For further information, please refer to the TOM of the data centre operator.
Building security (Hannover office)	The property boundary is marked by structural elements. The entrance can be accessed from 6:00 to 20:00; outside these hours, a key is needed. Access to the internal area (office entrance, reception area) is possible with a personal NFC chip. Access to the offices is controlled through doors, for which the NFC chip can also be used.
Accreditation (Hannover office)	Only registered, authorised personnel with a NFC chip can access the premises; all access is logged. Third parties are not admitted without authorisation, which can only be given by the management or CISO. Upon entry, visitor badges are issued, which must be visible at all times; in this way, unauthorised persons in the restricted area are identifiable. Visitors must agree to comply with data protection requirements. The office keeps visitor lists; third parties are required to identify themselves.
Access logging (Hannover office)	Access to the premises via NFC chip is only possible for authorized personnel who are registered by name, and accesses are logged. Third parties are not granted access without a registered visit and can only be authorized by a member of the management board or the CISO. Visitor badges are issued upon entry and must be worn visibly; unauthorized persons in the area to be protected are identifiable. Visitors are required to maintain privacy. Visitor lists are kept, strangers must identify themselves.
Alarm system (Hannover office)	The office of Hornetsecurity GmbH in Hanover is monitored outside office hours by motion detectors. The alarm is sent to a defined group of people.

Measures	Description
Building security(Berlin office)	The property boundary is marked by structural elements. The entrance, which is also guarded by a porter, can only be accessed from 6:00 to 20:00 using a token key. Outside these times, the entrance is closed. The internal area can be accessed with a personal NFC chip.
Accreditation (Berlin office)	The issued NFC chips are assigned by name; all access is logged. Third parties are not admitted without authorisation. Upon entry, visitor badges are issued, which must be visible at all times; in this way, unauthorised persons in the restricted area are identifiable. Visitors must agree to comply with data protection requirements. The office keeps visitor lists; third parties are required to identify themselves.
Access logging (Berlin office)	NFC log for the entrance area and visitor lists for the office area show who has accessed the respective areas and when.
2.2 Data media control	
Securing laptops	All Windows computers are equipped with a centrally managed antivirus client that cannot be deactivated. The operating system's own firewall is activated, and updates are installed automatically and promptly. Internal network: WLAN logon is performed via WPA2-Enterprise authentication. Access for guest devices is performed via the logically separated guest WLAN. If work is not carried out in the company's own office building, VPN to the data center must be used, as access to the relevant systems is otherwise not possible (IP blocking). The web filter service (proxy) must be used.

Measures	Description
Encryption of laptops	Laptops are naturally exposed to a higher risk of theft when used in changing environments. As a result, unauthorised persons may gain access to sensitive data. Access to hard disks is prevented by encryption; different approaches are permitted: - by activating the hardware-based SSD encryption in BIOS (OPAL SSC: AES 128/256bit encryption) - using hard disk encryption, e.g. Bitlocker with AES 128 / 256 bit, or VeraCrypt with AES, Twofish or Serpent, or dm-crypt/cryptsetup/LUKS with AES, Twofish.
Mobile data carriers	There exists a guideline for handling removable data carriers. Only data carriers that come from trustworthy sources are to be used for digital data exchange (procurement and issue by System Engineering). Private use of data media is prohibited. All Windows computers are equipped with a virus scanner that checks the data before it is accessed during read and write access. For external digital data medium exchange, sufficiently strong encryption of the data must be ensured, e.g. with VeraCrypt. External data exchange may only take place with the explicit, documented permission of the data owner. Data is only exported to mobile data media with documented customer request. Data exports are logged and can be traced. In the case of shipping, the shipping route must be permanently traceable (tracking ID).
Encryption of smartphones	There exists a BYOD policy for the use of private devices. Data on mobile devices may only be stored locally in Hornetdrive (encrypted) or on authorized cloud services. Authorization for the services takes place via personalized access.
2.3 Storage control	

Measures	Description
Rights management	User rights are restricted to the areas of activity (authorization matrix) according to the minimum principle. The assignment of rights is centrally controlled. Each user or his/her user profile is assigned to a department-dependent role, which makes available the necessary permissions on systems of the activities to be performed for his/her tasks (read, write, delete). The choice of system administrators is limited to those qualified for the task. Accesses are logged centrally.
Anti-virus software	For all Windows clients, a centrally controlled virus scanner is mandatory. The signature update interval is 60 minutes, heuristic detection is enabled. Users of Linux operating systems regularly perform offline scans. Mac computers are not subject to any obligation to use an antivirus scanner due to the operating system's security architecture. On Linux servers, the integrity of files is regularly checked by a host-based intrusion detection system (HIDS).
Firewall	Workstation clients: An operating system-side SW firewall is activated on all workstation computers. Communication with servers takes place via a centrally administered firewall that maps the requirements of data exchange between the systems and thus restricts communication to the necessary ports/services and, if necessary, IP ranges. Servers with increased protection requirements are located in a separate protection ring and can only be accessed via upstream proxies or load balancers with their own firewall. Weekly pen tests are performed to ensure that only the intended services can be accessed from outside.
Network disconnection	Servers at a site are separated by function-based VLANs. Servers with similar purpose are connected to each other in the same VLAN. The VLANs terminate in central firewall gateways. The configuration determines whether and to what extent internal networks can exchange data with each other.

Measures	Description
2.4 User control	
Creation of user profiles and roles	Access authorisations are restricted to the activity areas (authorisation matrix) in accordance with the principle of least privilege. Each user or their user profile is assigned to a department-based role, which reflects the authorisations needed to perform their tasks. The group / department heads work with the CISO to create the authorisation matrix and send it to the respective departments to assign authorisations. When an employee joins a department, the role and authorisation are determined based on the relevant matrix, and upon leaving the department, the authorisation is withdrawn.
External access using VPN	Connections to security or data protection relevant servers are only possible through a VPN tunnel (IPSec) from outside the company, to ensure that unauthorised persons cannot gain access in third-party Wi-Fi networks. Dial-up VPN access is personalised. The ciphers recommended by the BSI (German Federal Office for Information Security) for VPN are used.
2.5. Data access control (i.n.s.)	

Measures	Description
Authorisation concept	Access authorisations are assigned based on roles. For systems that cannot manage roles, authorisation levels are predefined that are requested, assigned, and rolled out for users. The group/department heads draft role authorisations and test them based on the scope of duties and document them in a matrix, which has to be approved by the CISO. Individual authorizations are documented for each system when they are assigned. The authorisation selected gives the users the minimum level of user rights that allows the employee to perform their tasks. Task changes or authorisation adjustments of a role lead to a review of the relevant authorisation matrix. As part of the onboarding process, the authorisations are requested from the group/department head and granted by the SE/IT department. During the offboarding process, the authorisations are withdrawn. Any reports of doubtful or undocumented assignments lead to a review of the relevant authorisation matrix and assignments.
Authentication using name/ password	Personal login credentials are used, partly with two-factor authentication using security tokens or additional one-time passwords.
Password policy	Passwords secure system access and are, therefore, at the centre of security requirements. Password policy: at least 10 characters, at least 3 of 4 criteria (upper case, lower case, number, special character). Different passwords must be used for different systems. For core systems, the password for administrative access must be at least 12 characters long. Critical systems (e.g. jump servers) use multi-factor authentication. The use of password management programs is recommended.
Traceability	Any change in data in a database is recorded in a transaction log. Transaction logging of any system changes is performed for the control panel. These are typically readable in an audit.

Measures	Description
2.6 Communication control	
Email encryption	Hornetsecurity offers all communication partners opportunistic transport encryption using STARTTLS in conjunction with Perfect Forward Secrecy (PFS). TLSv1.2 is used at least. To avoid communication problems, a ClientCertificateRequest is not always provided. For TLS encryption, algorithms are excluded that are marked "not recommended" according to BSI (German Federal Office for Information Security). With forced TLS, only "high grade" ciphers are permitted. With the "Archiving" service, the data is stored in unmodifiable encrypted form. It optionally supports email encryption with PGP and S/MIME. The signature algorithms and hash methods used for S/MIME certificates are based on BSI recommendations. For PGP, DSA & Elgamal with 2048 bit key length are used as encryption method.
VPN access	Connections to security or data protection relevant servers are only possible through a VPN tunnel (IPSec) from outside the company, to ensure that unauthorised persons cannot gain access in third-party Wi-Fi networks. Dial-up VPN access is personalised. IPsec enables the secure transmission of information in IP-based data networks, in a manner that ensures confidentiality, integrity and authenticity of the information transmitted via the IP protocol.
Documentation of recipient data	This makes it possible to trace where personal data was automatically transmitted to. Email transmission: The destination address is read out in detail from the customer configuration, based on DNS resolution for the target domain. The electronic data transmission is logged with date, time, message ID, sender, recipient, sending and receiving IP and where applicable, reverse DNS name and SMTP error code. The logs are erased in accordance with the erasure matrix.

Measures	Description
2.7. Input control	
Documentation of entries, changes and erasure of data	It is possible to trace who manipulated which data and when. Data entered, changed or deleted via the control panel (frontend) is logged on a transaction basis, including date, time, customer name, IP address and login name. Customers can only change data concerning them. Hornetsecurity employees can view and change all customer data. Under the applicable instructions, employees are required to enter or change modifications only at the customer's request or after consultation with the customer. The logs are erased in accordance with the erasure matrix.
Traceability of data processing	It is possible to trace which service manipulated which data and when. The analysis logs and, where applicable, data manipulation logs for spam and web filter services are stored centrally. Where necessary, access serves to ensure traceability of data processing. The logs are erased in accordance with the erasure matrix.
2.8 Transport control	

Measures	Description
Diligent selection of transport personnel	Ensuring that the confidentiality and integrity of personal data are protected during transport of personal data. Personal data are only transmitted in an encrypted form. The purpose is to ensure that the delivery can be tracked (tracking number of the carrier). Reliable, local freight forwarders are contracted to carry out the delivery. In the case of national or international orders, the consignment must be tracked at all times, even if it is transferred to other carriers or subcontractors. Data carriers are shipped in suitable outer packaging that protects them against mechanical damage. Data are held on-site as a backup until the consignment has been received/ receipt has been confirmed.
Encryption of data media	Ensuring that the confidentiality and integrity of data are protected during transport of data carriers. With respect to external digital data medium exchange, a sufficiently strong encryption of data is used, e.g. using VeraCrypt or 7zip. An external exchange may only take place with the explicit, documented permission from the data subject.
2.9. Ability to restore availability and access to data	

Measures	Description
Type and scope of data backups	The SE/IT department is responsible for the correct operation, follow-up of system notifications and the configuration of data backups. The department uses open source software for this purpose. The backup is a combination of full and incremental backup. The data are backed up automatically at least every 24 hours. Data versions for at least the past 30 days are available. The backup is carried out centrally for each data centre by local agents through the internal Gigabit network using RAID hard disks on a backup system. As a result, the restore process can be started within a few minutes. The backup systems themselves back up each other across the data centres. The servers that have been backed up or will be backed up are documented in the Wiki. Erasure periods are laid down in the erasure matrix.
Recovery policy	The SE/IT department is responsible for the correct operation, follow-up of system notifications and the configuration of data backups. The department uses open source software for this purpose. In the event of a fault, the operating system, configuration and data can be uploaded to an existing or newly assembled system through partially or fully automated installation (data restore and / or automated deployment) (including the backup system itself). Regular, documented test restores take place. If the required recovery time falls below certain trigger values, the following additional measures are taken to ensure the availability of the systems: - < 24 hours: a second system for failover operation is provided, - < 4 hours: a cluster is operated.
2.10 Data integrity	

Measures	Description
Performance tests of new processes	- Specification of functional and non-functional new projects using a customised version of the Volere template. - Code reviews of all changes before going live for quality assurance purposes - 4-eyes principle for all changes to live systems - Unit tests for automated testing of atomic functions and for improving the maintainability of the source code - Automated, standardised integration tests for each release (Selenium WebDriver toolkit using BrowserStack or Docker Container, CI Pipeline) - Extension of the test cases after implementing new functions against the specification; finding and fixing bugs - After each release, automated tests are rerun.
Measures to protect the integrity of personal data	Changes to authorisation and configuration objects and personal data can be made using the control panel. Each action - including a (failed) login - is stored in the audit log with date, time, login name, action, object and original IP address. Three standard authorisation roles are predefined (user, customer administrator, partner) for authorisation administration purposes. Individually definable authorisations, which are also made available as roles, are possible. Users are assigned to these roles. Data are transmitted solely through encrypted connections (VPN or TLS, compare section 2.6). Data transmission from tier 1 (front end) to 2 or tier 2 to 3 (back end) are only possible for defined endpoints using firewall rules.
2.11 Processing control	

Measures	Description
Order execution	- The contractor's employees are regularly trained to perform the service in accordance with the service agreement concluded with the client (taking into account the associated DPA). - There are familiarization processes and boot camps for new employees. - The issuer and recipient of instructions are explicitly named. - Instructions are only carried out after written issuance / written confirmation (via ticket system). - Processes, especially for data protection-relevant procedures, are described in the wiki, including escalation paths. There is a clear communication channel for data protection requests.
Selection of data processors who comply with GDPR requirements	The purpose of processing control is to ensure that data processing is carried out in accordance with instructions. Processors are evaluated and selected based on qualifications and reference customers, certificates and security concepts. When a contract is awarded to the processor, the points required under GDPR are laid down in the contract. If the contractor is unable to meet these requirements, the contract will not be concluded.
Conclusion of GDPR-compliant processing agreements	A processing agreement must cover all the essential aspects. Hornetsecurity as client only concludes GDPR-compliant processing agreements with service providers. If applicable, the DPO will be involved in the review of DP-agreement.
Ensuring the erasure of data after the end of the contract	Upon entry into force of the GDPR, the provisions on the erasure of personal data represent an improvement compared to the previous legal situation as the relevant provisions have been formulated in more detail and in some cases even go beyond that. If there is no other legal basis, the periods specified in the erasure matrix apply to the erasure of personal data. There is an adequate process for erasure requests.

Measures	Description
Ongoing checks of service providers	Hornetsecurity attaches great importance to the documentation and implementation of data protection and IT security processes for service providers. It reviews documentation and performs random on-site inspections. It only enters into contracts with service providers if they give and undertake to comply with confidentiality and data protection requirements.
3. Availability control	
Disaster risk management	Disaster risk management is divided into 3 areas: Measures to mitigate the risks, impact and occurrence of damage/loss. 1. Hornetsecurity uses at least two data centre locations in Germany far apart from each other, which are run by certified operators. Each of these data centres has its own redundant power supply, network supply, air conditioning and extinguishing systems. Data processing is fully guaranteed by operating just one data centre. The second and additional data centres are used to increase redundancy. In addition, central data systems are equipped with automatic replication and hot failover functionality. Data is stored in a geo-redundant manner. Communications and data exchanges are always encrypted. 2. Data is always stored on mirrored disks using adequate RAID processes. Data is backed up regularly in accordance with the backup plan in order to restore older versions of data. Important services are provided by clustered servers. A Wiki with current configurations and intended use is maintained for all servers. Documented catastrophic incident simulations take place on a regular basis. 3. The criticality of the servers and services is documented with the expected maximum recovery time, which determines the priority in a disaster recovery.

Measures	Description
Emergency/ catastrophic incident	As part of the IT security strategy, IT emergency management has the task of ensuring the continuity of business operations. The criticality of the servers and services is documented. This is used to determine the order of recovery. Services and hardware are subject to comprehensive monitoring. For different events (warning, malfunction, failure) there are escalation plans with roles and persons to be notified. In the case of a complete failure, hardware equipment and individual parts in different configurations are available for different purposes. Used configurations are documented centrally. In the event of a fault, the operating system and configuration can be uploaded to a newly assembled system through partially or fully automated installation (data restore and / or automated deployment). There are catastrophic incident exercises and possible catastrophic scenarios are identified. The results are documented and serve as a basis for regular improvements.
4. Separability	

Measures	Description
Separation between product and test systems	For internal purposes (e.g. development, testing and backup), logically and physically separate systems with their own database and data structure are used. New versions are subject to a multi-level quality assurance process. Automated software tests perform standard tests and guarantee the correct operation of all core functions. After the completion of these standard tests, which are performed automatically, they are run in a test environment that can only be accessed by internal employees and external beta testers obliged to comply with data protection requirements. The test duration in the testing environment is at least 1 week. A feedback process adapts the automated standard tests in case of errors for future standard test procedures. After an error-free test phase, the new version is rolled out in live operations.
Assignment of database access permissions	Users get access to different amounts of data and query options based on a predefined role concept. Standard roles are available for assignment, starting with the user role, which allows users to see their own data based on the logged-in user's account, through to the partner role, which gives partners access to information on customers and users assigned to them and whose roles they can also configure, create or erase. Individual roles can also have differentiated access authorisations; these can be assigned to any user account.
Logical customer separation	Logical customer separation is set up with a view of ensuring that customers (cloud users) cannot view information from other customers (cloud users). As a result, customers cannot access the resources of other customers, in particular, virtual machines, networks or cloud storage. in the control panel, logical client separation is performed at the database level.
5. Organisational control	

Measures	Description
Appointment of a suitable data protection officer	Lukas Wagner, LL.M. Cert. Data Protection Officer (TÜV) HK2 Comtection GmbH Hausvogteiplatz 11 A 10117 Berlin Telephone: +49 30 278900180 https://www.comtection.de As an external data protection officer, Mr. Wagner assumes the rights and obligations, e.g. monitoring the processing operations, checking the compatibility with the data protection laws, representation before the supervisory authorities. He has a long-standing experience in the field of data protection. The company offers the specialist knowledge on monitoring required by law as a matter of course, documentary evidence of which can be provided to third parties.
Implementation of regular review and evaluation cycles	An internal reporting process encourages all employees to escalate any identified irregularities. The IT security officer (CISO) accepts the information and adjusts existing processes in liaison with the relevant group leaders. Employees are given feedback on any reported issues. The CISO performs random checks of authorisation policies and technical and organisational protection measures to identify optimisation opportunities. Regular checks and any adjustments to the measures are carried out to ensure that they still comply with the latest technology standards. Regular network scans check for any instances of unauthorised service provision. Changes in operating procedures or in relevant processes are communicated across the company. Active incident management with regular group leader meetings addresses shortcomings that have resulted in faults and is used as a basis for (technical and organisational security) measures to ensure authenticity, integrity, confidentiality, availability and binding nature of all systems in the long term.

Measures	Description
Preparation of an erasure policy	Hornetsecurity distinguishes between different types of personal data for each service. A detailed matrix for rule deletion time limits is provided in the erasure matrix, which can be requested separately. Erasure in special situations, which are not covered by rule deletion time limits, is carried out on a case-by-case basis together with the department responsible for data storage. The IT security officer has the lead responsibility; in the alternative, this can be the data protection officer. Suspension of erasure - especially in the case of archived emails - is possible at the request of the customer or an authorised body. In order to be able to fulfill deletion requests from data subjects, early deletion of data in the archive is possible. This process can be triggered in self-service by authorized customer personnel. The deletion actions are logged. If data is stored for periods exceeding the time limits specified in the matrix for rule deletion time limits, this is done anonymously by cumulating the sets of data.
Instructions / training	Employees (including trainees, student assistants) regularly receive written instructions regarding data protection requirements and are required to confirm this by signature (once every six months). Test phishing e-mails are sent out at irregular intervals per department for mandatory awareness training. Training videos and awareness exercises are rolled out on various topics. A company-wide awareness score provides information about the success.
Scope of responsibilities	Assignment of responsibility for information, applications and IT components - Provision of services to the customer: SD (service desk) - Internal service provision: SE/IT (systems engineering/infrastructure team) - Monitoring: SE/CM (systems engineering/cloud management) - Programs & scripts: SE/SL (systems engineering/security labs) - Front / backend, data storage: PDC (programming and developing centre) - Process coordination & IT security: CISO (chief information security officer) - Faults and their consistent elimination: IM (incident manager)

Measures	Description
Queries from data subjects	The GDPR provides for a right of access and information for data subjects (Article 15 GDPR) Requests for information shall be sent by email to datenschutz@hornetsecurity.com or privacy@hornetsecurity.com. The request is recorded in the ticket system and the receipt is confirmed promptly. The information is provided free of charge. In cases of unfounded or excessive requests by an interested party, the provision of information can be denied. There is a detailed process for requests (summarised): 1. Verification whether the request is at all a request for information. 2. Verification of the identity of the initiator. 3. Verification whether personal data of the data subject have been processed. 4. If there is no data: Answer in the negative sent to the data subject. 5. If there is data: Compilation and prompt response within one month of receipt. Where the time limit has been extended, the initiator is promptly notified. In addition, the GDPR provides for the rights to information (Art. 13 + 14 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR) and data portability (Art. 20).

Measures	Description
Disposal policy for data carriers	Data carriers on which customer data was once stored are not returned for a refund if defective, and are instead sent directly to be destroyed. Data carriers on which customer data was stored are also never reused. Data carriers earmarked for destruction are collected under lock and key in SE. Data carriers are professionally destroyed by a certified provider, contracted by Hornetsecurity as needed. The data carrier destruction is monitored and logged. If the data carriers to be erased are servers used abroad with built-in data carriers, the following applies: - All personal data, configurations and scripts for services are erased - A wipe program is installed and run - Customers are asked to dispose of the server for Hornetsecurity on site.
Document versions	Date
0.1	26.03.2018
0.2	25.05.2018
0.3	08.08.2018
1.0	14.08.2018
1.0.1	13.01.2020
1.1	06.01.2021
1.2	01.05.2022
1.2.1	06.07.2022

Annex 3: Authorized subcontractor(s)

COMPANY	ADDRESS	SERVICE	TRANSMISSION BASIS [1]	NOTE
HORNETSECURITY LIMITED (MALTA)	Block LS3, Level 1 Life Science Park San Gwann Industrial Estate San Gwann, SGN 3000 Malta	VM Backup & 365 Total Backup		
DOCUSIGN	221 Main St., Suite 1550 San Francisco CA 94105, USA	Electronic agreement management	SCC	No data transmission for core services
HKN GMBH	Hochstadenstraße 5 47829 Krefeld Germany	Colocation		See note [2]
HORNETSECURITY GMBH	Am Listholze 78 30177 Hannover Germany	Internal Subcontractor for Core Services		Only applies if the contractual partner is "Hornetsecurity Iberia S.L", "Aegis Security Argentina S.A.", "Hornetsecurity Inc." or "Hornetsecurity Ltd."
HORNETSECURITY INC.	6425 Living Place Suite 200 Pittsburgh, Pennsylvania 15206, United States	Internal subcontractor for Service Desk, Customer Support	UK Standard Data Protection Clauses	Only applies if the contractual partner is "Hornetsecurity Ltd. (UK)"
HOSTWAY DEUTSCHLAND GMBH	Am Mittelfelde 29 30519 Hannover Germany	Colocation		See note [2]
IT-SEAL GMBH	Hilpertstr. 31 64295 Darmstadt Germany	Security Awareness Training		
MK NETZDIENSTE GMBH & CO. KG	Marienwall 27 32423 Minden Germany	Colocation		See note [2]
PIN MAIL AG	Alt-Moabit 91 10559 Berlin Germany	Postal Services		
QUALITYHOSTING AG	Uferweg 40-42 63571 Gelnhausen Germany	Hosted Exchange		

[1] BCR = Binding Corporate Rules, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116
SCC = EU standard contractual clauses

[2] Hornetsecurity operates its infrastructure in an external data centre. However, it is contractually, technically and organizationally ensured that any access to Hornetsecurity's data by the computer center operator is excluded.

COMPANY	ADDRESS	SERVICE	TRANSMISSION BASIS [1]	NOTE
SALESFORCE.COM INC.	The Landmark @ One Market Street San Francisco CA 94105, USA	Customer-Relationship-Management	SCC	No data transmission for core services
SKYFILLERS GMBH	Schiffbrücke 66 24939 Flensburg Germany	Hosted Exchange		
TWILIO INC.	375 Beale Street, Suite 300 San Francisco California 94105, USA	SMS Communication	SCC	

Annex 4: Amendments to the text of the contract

. / .