Valid from:	01.06.2016
Valid till:	01.10.2028
Next review:	01.10.2027
Responsible person(s):	Olaf Petry, CISO
Confidentiality	Public

Data protection information

Managed Security Services

Hornetsecurity Group

Data protection information for the offered services

I. Introduction 3

1. Base 3
2. Contact information 3

II. General information about data processing 5

1. Scope and purpose of processing personal data 5
2. Legal basis for processing personal data 5

III. Data processing for the operation of the *services* 6

1. Basic data 6
   a. Master data 6
   b. Configuration data 6
2. 365 Permission Manager 7
3. 365 Total Backup 7
4. 365 Total Protection 8
5. 365 Total Protection Enterprise Backup 9
6. AI Recipient Validation ..... Fehler! Textmarke nicht definiert.
7. Control Panel, login on 11
8. Hornet.email Webmail, login on 11
9. Hosted Exchange 12
10. AI, use of artificial intelligence 12
    a. Introduction 12
    b. Purpose of the processing 12
    c. Data we collect 13
    d. AI tools, data storage and retention 14
11. Security Awareness Service 15

12. Spam and Malware Protection 16
a. Optional: Advanced Threat Protection (ATP) 16
b. Optional: E-mail Encryption 16
c. Optional: Archiving 17
d. Optional: Continuity Service 18
e. Optional: E-mail Signature and Disclaimer 18
f. Optional: E-Mail made in Germany 18
13. Test Onboarding 19
14. VM Backup 19
15. Web Filter 19
16. Websafe, privacy policy for third parties 20
IV. Right of objection and removal 21
V. Rights of data subjects 21
VI. Recipients of data 22
VII. Data transfer to third countries 22

I. Introduction

1. Base

Effective data protection is based on comprehensive information about the collection, processing, and use of your data ("data processing"). We would therefore like to inform you about the following:

- when or during which activities we process data,
- what data we process and for what purposes,
- who receives data,
- your rights regarding our processing of your data.

This privacy statement relates only to the use of personal data in the context of the services. You can download this privacy statement permanently and at any time at https://www.hornetsecurity.com/service-privacy-statement/

2. Contact information

As defined by the General Data Protection Regulation (GDPR), the customer is always the controller, i.e. responsible for data processing as part of the services. Hornetsecurity acts as the processor as defined by Art. 28 GDPR. Some of the services are also provided by other Hornetsecurity Group companies as subcontractors:

	Processor	The services are provided in an internal subcontracting relationship by
☐	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com	-/-
☒	Hornetsecurity Iberia S.L Calle Vía de las Dos Castillas 33, Edificio 3 Ática 3 Planta Tercera D 28224 Pozuelo de Alarcón, Madrid España Phone: +34 91 368 77 33 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Argentina S.A. Belgrano 53 Piso, PB Dpto: B Tandil, Buenos Aires Argentina Phone: +54 9 249 449 9296 E-mail: info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com

	Processor	The services are provided in an internal subcontracting relationship by
☐	Hornetsecurity Ltd. 82 James Carter Road Mildenhall, Bury Saint Edmunds IP28 7DD United Kingdom Fon: +44 203 0869 833 Email: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Ltd BLK LS3, Level 1, Malta Life Sciences Park San Gwann Industrial Estate San Gwann, SGN 3000 Malta Phone: +44 203 0869 833 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 United States Phone: +1 412 924-5300 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Canada Inc. Suite 500, Park Place Building 666 Burrard Street, Vancouver, BC V6E 3P3 Canada Fon: +1 (514) 527-3232 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	IT-Seal GmbH IT-Seal GmbH Hilpertstr. 31 64295 Darmstadt Germany Phone: +49 (0) 6151 493 8990 E-Mail: kontakt@it-seal.de	Hornetsecurity GmbH Am Listholze 78 30177 Hanover Germany Phone: +49 511 515 464-0 E-mail: info@hornetsecurity.com

We have also appointed a Data Protection Officer. You can contact this officer at privacy@hornetsecurity.com.

II. General information about data processing

1. Scope and purpose of processing personal data

The provision of the services requires the processing of various types of data. In addition, the scope of data processing depends on your use of the functionalities of the services, for example which data you process or have processed there or for which data you consent to data processing.

As part of the contract established with Hornetsecurity for the use of the services, you are obliged to provide the personal data required for the fulfillment of the contract. Refusal to provide this data may constitute a breach of duty, which may lead to your being liable for damages. You are not obliged to provide us with personal data. However, if providing this data is technically necessary for the use of our services, a refusal will mean that you will not be able to use our services.

When using the services, you are not subject to automated decision-making as defined by Art. 22 GDPR.

2. Legal basis for processing personal data

The legal basis for the processing of personal data is presented below.

Processing reason	Legal basis in the GDPR	Explanation
Fulfillment of the contract or implementation of pre-contractual measures	Art. 6 (1) (b)	Processing is only carried out to the extent necessary for the exercise and fulfillment of the rights and obligations arising from the contract. Unless expressly stated otherwise, we only process data to this extent.
Legitimate interest	Art. 6 (1)(f)	Processing takes place insofar as we have a legitimate interest and no conflicting overriding interests of the data subject are apparent. The specific interest is explained in this data protection information as part of the processing description.
Legal obligation	Art. 6 (1) (c)	Processing takes place insofar as this is necessary to fulfill German or European legal obligations.

III. Data processing for the operation of the *services*

In order for us to provide you with the *services*, it is necessary to process certain data.

The legal basis for the processing of this information and stored data is the necessity for fulfilling the existing contractual relationship. The storage period is therefore generally based on the duration of the contractual relationship. However, alternative legal bases, such as statutory retention periods, may apply after the end of this period.

1. Basic data

The entity of the Hornetsecurity Group marked under I, "Contact information" (page 3**Fehler! Textmarke nicht definiert.**), is responsible for processing the master data and configuration data

a. Master data

The client's master data (name, address, contact person, telephone number, e-mail address, department, position, booked services, billing period, account details) is collected for the administration of the services and used to provide the contractually agreed services. Personal data of co-users (e-mail address) is collected and used to provide the contractually agreed services.

Data processing of co-user data takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

The client's master data is processed for the purpose of customer master data management by subcontractors on systems in a third country (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). The data is transmitted on the basis of standard contractual clauses.

Data processing in Salesforce's CRM software is carried out under joint responsibility in accordance with Art. 26 GDPR of the companies named under I, "Contact information". Data subjects can view the main contents of this agreement on request. The legal basis for this is our legitimate interest in accordance with Art. 6 (1) (f) in conjunction with Recital 48 GDPR in increasing efficiency and minimizing costs by creating and using joint administrative structures.

Furthermore, parts of the client's master data are transmitted to subcontractors within the EU for the purpose of mailing and sending invoices (by letter or e-mail) and processed on their systems (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Germany).

b. Configuration data

The technical configuration of the booked *service* is stored in connection with the user's e-mail address, the group membership of a user or the customer's domain name.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). Apart from the contractor and designated representatives of the client, no third parties have access to the data.

The following applies additionally to VM Backup and 365 Total Backup:

To validate the license, the master data required for definitive identification (e-mail address) is transferred to the systems of Hornetsecurity Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malta, EU.

2. 365 Permission Manager

365 Permission Manager is a Governance, Risk & Compliance (GRC) software tool that gives users a complete overview and understanding of their M365 file permissions in their own tenant in the Microsoft Azure Cloud for SharePoint Online, OneDrive for Business, Microsoft Teams and Microsoft 365 Groups.

Automatic data processing includes retrieving and processing the metadata of the objects stored in the M365 tenant. Objects whose metadata is retrieved are: Files, folders, document libraries, sites, users, groups. Retrieved and processed metadata includes the owners of the objects (e-mail address, display name), information on the objects to which access rights have been granted (e-mail address, display name, both from objects within and outside the own organization), as well as the assigned permissions.

Access to the contents of the objects (file contents) is not possible.

The retrieved and stored metadata is deleted as soon as the corresponding object is deleted in the Microsoft Cloud or when the service is deactivated for the customer in the Control Panel.

The retrieved metadata is processed on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

3. 365 Total Backup

365 Total Backup is a reliable, intuitive and easy-to-manage backup and recovery solution for Microsoft 365 mailboxes, OneDrive for Business accounts, SharePoint document libraries, Teams chats and endpoints.

365 Total Backup provides the customer with a policy-based configuration, overview and monitoring of rights, backups and M365 objects to be backed up via a multi-tenant console. All backup data is encrypted with customer-specific AES-256 keys.

The data management of the secured and encrypted data is carried out within the Hornetsecurity Group by Hornetsecurity Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malta ("Hornetsecurity Ltd.").

The encrypted backup data is stored in accordance with the configuration set by the customer:

- in the Hornetsecurity cloud, amongst others in Germany, France, Switzerland, the United Kingdom, Canada and the United States (Virginia and Georgia), provided by Hornetsecurity GmbH, Am Listholze 78, 30177 Hanover,
- or, for older installations (prior to February 2022), in the Microsoft Azure Cloud, Western Europe zone – as 'cold storage', with Hornetsecurity Ltd. utilising the Microsoft Azure platform and compliance services. The Azure Western Europe cloud platform

and services are certified to SOC 1 Type 2, SOC 2 Type 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS and HIPAA.

During operation, the software license used is compared online with the purchased license stored in the master data. The contractor does not transfer or process the usage data of the services.

4. 365 Total Protection

With Spam and Malware Protection, the client's incoming e-mails are filtered for harmful content (e.g. viruses), unwanted advertising (e.g. spam) and legitimate advertising (e.g. newsletters) on the contractor's IT systems. Outgoing e-mails are also filtered.

Automatic data processing includes the metadata of the message transmission (e-mail address of the sender and recipient, e-mail subject, date/time of e-mail receipt and delivery, IP addresses of the servers involved in the communication, SMTP error code and text), the content of e-mails and the classification of the e-mail (clean, spam, virus, infomail). The message metadata is used for display in the Control Panel and is deleted after 14 months at the latest. The e-mail itself is deleted after successful delivery or bounce.

The use of individual user signatures, company disclaimer and 1-click intelligent ads requires the use of a directory service on the part of the client, which can be queried by the contractor via the LDAP protocol. In addition, the groups from the user directory must be organized in the Control Panel. The messages must be sent via the contractor's relays.

Automatic data processing includes the user's e-mail address, assigned group name in the directory service, other information that may be linked in the directory service such as organizational affiliation, position, telephone number, fax number and e-mail footer content that is assigned to the group in the directory on the client's side. The personal data extracted from the directory will be deleted after the end of the use of the service. The processed message is deleted after successful delivery or bounce.

Global S/MIME & PGP Encryption: The contractor encrypts and signs outgoing e-mails and decrypts incoming e-mails of the client on its own IT systems in accordance with the set guidelines. Depending on the guideline settings, outgoing e-mails are made available to the recipient in the protected Websafe.

The automatic data processing includes the e-mail address of the sender and recipient, private and public S/MIME or PGP key, outgoing e-mail content to third parties (Websafe), e-mail address in public keys of third parties, encryption status and contents of e-mails. The sender, recipient and encryption status data are used for display in the Control Panel and are deleted after 14 months at the latest. The e-mail itself is deleted after successful delivery or bounce.

Archiving: The contractor archives the client's e-mails in a tamper-proof manner on its own IT systems.

The automatic data processing includes the e-mail address of the sender and recipient, e-mail subject, date/time of e-mail receipt, IP addresses of the servers involved in the communication, the content of e-mails and, if applicable, the name and type of attachment.

The data of the sender and recipient address, e-mail subject, date/time, attachment name and type are used for display in the Control Panel. All this data, including the message itself, is

stored for a customer-specific archive period plus 1 year and then deleted. A deletion suspension at the customer's request can increase the storage period.

Advanced Thread Protection (ATP): protects the client's e-mail traffic against targeted and individual attacks such as spear phishing, blended attacks, advanced persistent threats, ransomware and CEO fraud. In order to detect attacks, the contractor uses advanced filtering techniques to examine e-mails of the client that are classified as suspicious.

For this purpose, meta-information on the e-mail content and the e-mail attachment type, name and -content are processed automatically. The meta-information on the e-mail content is used for display in the control panel and is deleted after 14 months at the latest. The e-mail is deleted from the ATP system after successful analysis.

Contingency Covering: In the event of a failure of the target server, the contractor shall provide each user with an e-mail mailbox with 10 GB of storage. Authorized users can access e-mails in this mailbox via a webmail interface or via IMAP and POP3.

Automatic data processing includes message metadata (the e-mail address of the sender and recipient, date/time of e-mail receipt), e-mail content and webmail metadata (login name, IP address, connection duration, retrieval volume, protocol). Message metadata, webmail metadata and archived messages are deleted after 14 months at the latest. Messages in the webmail mailbox are deleted at the latest when the customer no longer uses the service.

Data processing takes place on dedicated hardware, located in leased data centers (colocation).

For the use of single sign-on, the e-mail address is forwarded to Microsoft when the user logs in.

Other data will not be passed on to third parties, nor will third parties access the data.

5. 365 Total Protection Enterprise Backup

This service is a merger of the services

- 365 Total Protection (page 8) and
- 365 Total Backup (page 7).

Please read the relevant information provided there.

6. AI Cyber Assistant: AI Email Security Analyst

AI Email Security Analyst advises end users on the precautions they should take when dealing with the reported email. The feature also provides an explanation and assessment of indicators of legitimacy or malicious intent within the message.

Administrators can use the AI Email Security Analyst in Email Live Tracking, where they receive on-demand generic analysis, risk assessment and AI-powered classification of email content. No detailed information regarding the email content is disclosed.

The AI Email Security Analyst processes data via pre-trained LLMs hosted in isolated Microsoft Azure environments. MS Azure servers in the US region for customers in the US and Canada; MS Azure servers in the Europe region for customers in the EU and the rest of the world.

Following assessment, the email content is neither stored in the AI system nor used for training purposes. The assessment output, in conjunction with user feedback from the AI Email Security Analyst, may be used to improve the detection algorithms.

The emails are stored on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

7. AI Cyber Assistant: AI Recipient Validation

AI Recipient Validation is a tool that allows end users of M365 tenants to be alerted in their Outlook client when an e-mail they sent may be misdirected (e.g. if an incorrect recipient was added to an e-mail thread) or contains sensitive information (e.g. credit card numbers or personal data). Users can accept the suggestions or continue without making any changes to the e-mail. The product's suggestions are updated based on user behavior.

Automatic data processing in the cloud includes the subject of the e-mail, sender and recipient (plain text name and e-mail address in each case), type of e-mail (new, reply, forwarded), time the e-mail was sent, language set for the Outlook client, all users and groups of the tenant, number of recipients in distribution lists, number of e-mails sent, as well as performance statistics for the Outlook add-in.

Automatic data processing in the local Outlook client includes the e-mail content.

AI Recipient Validation uses neither generative AI nor large language models (LLMs). The assessment is based on rule-based decision logic in the form of a decision tree. Feedback regarding whether a recipient has been confirmed as valid or unwanted in the respective email context can be used to adapt this decision logic and thus improve future assessments. Neither training nor fine-tuning of an LLM takes place in this process.

Data processing takes place on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

8. AI Cyber Assistant: Conversational Agent

The Conversational Agent can be accessed via the Control Panel and supports users at partner level and those authorised to use the agent. It provides answers to questions relating to sales, technical matters, and usage and performance metrics for the services.

The Conversational Agent uses a pre-trained Large Language Model (LLM). To answer enquiries, the model is granted access to selected internal sales, marketing, technical and support information, as well as – within the user's authorisation context – relevant customer and usage metadata from Email Live Tracking.

Input and output data are processed as context at runtime and are not used to train the LLM.

For quality assurance purposes, the last 50 user inputs and LLM outputs are stored for a maximum of 30 days.

Please note that the responses are generated by AI and may not always be correct.

Data processing takes place on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

9. AI Cyber Assistant: Teams Protection

Teams Protection safeguards end users from harmful messages whilst exchanging messages in Microsoft Teams by scanning all messages containing URLs. If a threat is detected, a warning message appears in the chat history via the AI Cyber Assistant bot. Optionally, messages containing potentially malicious URLs can be deleted. Teams Protection utilises the database and detection technologies from Hornetsecurity's Secure Links (part of Advanced Threat Protection, page 16).

Administrators receive an overview in the Control Panel of chats containing detected malicious URLs, including details of the participants involved and the URL in question. Accounts that distribute malicious content can be blocked.

All Teams messages are processed on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

10. Control Panel, login on

If you are already a Hornetsecurity customer, you can use our website to log in to the Control Panel, from where you can use and manage your service. To log in, you will need your user name or e-mail address and your password. The storage period is therefore generally based on the duration of the contractual relationship. However, alternative legal bases, such as statutory retention periods, may apply after the end of this period.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

The legal basis for the processing of this information and stored data is the necessity for fulfilling the existing contractual relationship.

11. Hornet.email Webmail, login on

If you are already a Hornetsecurity customer, you can use our website to log in to the Control Panel, from where you can use and manage your service. As a Webmail customer, you can log in via a separate link in your mailbox. To log in, you will need your user name or e-mail address and your password. The storage period is therefore generally based on the duration of the contractual relationship. However, alternative legal bases, such as statutory retention periods, may apply after the end of this period.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

The legal basis for the processing of this information and stored data is the necessity for fulfilling the existing contractual relationship.

12. Hosted Exchange

In addition to Spam and Malware Protection, the client can book Hosted Exchange mailboxes if no own e-mail server is to be used. Hosted Exchange offers you the secure operation of a professionally managed exchange server in your e-mail domain with Active Sync, shared contact information, online calendars, group collaboration and access from different clients and hardware platforms without any additional effort.

Automatic data processing includes e-mails received and sent, the user's e-mail address, group memberships, mailbox creation date, authorizations from/to other internal accounts in the same domain and mobile devices used to access the mailbox. Furthermore, if entered: Company, position, department, employee number, supervisor, telephone numbers, address. The data will be deleted no later than 90 days after termination of the service.

E-mails are transmitted to servers of subcontractors in the EU for processing and storage (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Germany or Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Germany).

The legal basis for the processing of this information and stored data is the necessity for fulfilling the existing contractual relationship.

13. AI, use of artificial intelligence

a. Introduction

This document explains our practices regarding the collection, storage and processing of e-mail metadata and latent topics from e-mail content for our machine learning and AI projects at Hornetsecurity. Our approach prioritizes user privacy and is in line with existing data protection guidelines. While our primary focus remains on e-mail metadata, identifying e-mail topics provides insights for refining machine learning models, particularly for e-mail classification, which is required for services such as Targeted Fraud Forensics, Phishing Protection, AI Recipient Validation and Infomail Filtering products and features.

b. Purpose of the processing

Continuous improvement of models for classifying e-mails

We refine and improve machine learning algorithms by using e-mail data to ensure the accuracy and relevance of their predictions. This helps us to effectively distinguish between genuine communication, spam and malicious content.

E-mail categorization

E-mail metadata and latent topics are used to categorize e-mails into different types, such as "advertising" or "phishing". This approach is closely linked to our Infomail Filter product, which allows users to quarantine unwanted e-mails.

Sharing sensitive information and data leaks

For our Targeted Fraud Forensics and AI Recipient Validation products, it is crucial to predict the likelihood of sensitive information being passed on to unauthorized persons. To this end, we analyze e-mail metadata, social graphs, e.g. connections between e-mail senders and recipients, and latent topics to identify potential data leaks and security threats.

Improving user-friendliness

User actions, such as reporting unwanted e-mails or changing e-mail content based on suggestions, influence the optimization of the user experience of Hornetsecurity's products. This optimization reduces unwanted e-mails and offers more relevant warnings and recommendations for action.

Account protection and security

Evaluating e-mail data and analyzing trends to detect anomalies or potential security threats, such as emerging phishing campaigns or compromised e-mail accounts, helps us to protect our users and their data.

c. Data we collect

Basic identifiers:

- E-mail address of the sender
- E-mail address(es) of the recipient
- IP addresses, host names and ASN (Autonomous System Number) of the sender servers

Temporal data:

- Timestamp of e-mail deliveries
- Timestamp for feedback from users and administrators on e-mails that have been reported as spam, infomail or harmless
- Message characteristics and authentication status:
- Size of the message
- Message format (HTML, plain text and other content type details)
- The checksum(s) of the body and header of the message
- Authentication and verification details (entries for DKIM, DMARC, SPF records)

Interaction information:

- Feedback on the e-mail (e.g. reported as spam or harmless)
- Response actions to messages (e.g. answered, forwarded, first contact)
- Actions in response to alerts and notifications (e.g. deciding whether to send an e-mail after being prompted by AI Recipient Validation)
- Metadata such as the number of messages, keywords in the subject and the distribution of the associated timestamps for specific recipients / distribution lists (AI Recipient Validation)

Metadata of attachments:

- Number of attachments
- File types (e.g. .pdf, .docx, .jpg)
- File sizes
- File names with anonymized personal data
- Checksum(s) of the file(s)

Links and domains:

- Links in an e-mail or in e-mail attachments with anonymized URL paths and parameters
- Domains of the extracted links and their DNS information (e.g. A records of the DNS)

Header data:

- Information from the header section of the e-mail, including:
- From
- To
- Date
- Subject with anonymized personal data
- Message ID
- User agent and X-Mailer data
- Received lines
- Results of the authentication
- Content-related message headers (e.g. "Content-Type")

Derivation of the topic from the body of the message:
To improve our e-mail classification models, we extract the general topic of the e-mail content. The message text is processed to recognize a superordinate category or topic without storing specific or sensitive details from the message text itself.

Example: An e-mail with details of an upcoming sale of goods could generally be categorized as a "promotion" or "sales event".

d. AI tools, data storage and retention

All AI tools and models are either developed in-house or provided via trusted platforms such as Azure. For AI storage, we use both our own infrastructure and Large Language Models (LLMs) hosted by Microsoft Azure to provide advanced AI capabilities. Our prompt data contains only the minimum personal data necessary to provide the service. The data is never stored or used for model training without explicit permission. External LLMs are trained without our data by the LLM provider.

The AI storage and processing infrastructure is located either in the Hornetsecurity data center or in Azure's secure cloud environment. Access to data and models is strictly controlled and monitored under data protection law. Third parties or unauthorized personnel are not granted access to this data. The machine learning models are provided and used exclusively via our secure infrastructure or via secure connections to Azure services. Every data transaction between customer systems and our AI/ML API is protected by robust end-to-end encryption procedures. This ensures the confidentiality and integrity of the data during transmission.

Protocols for storage and retention

- The data is encrypted at rest and during transmission. The encryption procedures comply with industry best practices.
- The data is stored for as long as is necessary to fulfill the stated processing purposes. Some log files may be retained for up to 12 months in accordance with our data retention guidelines.

- All other data stored for the operation or fulfillment of the functions of an active paid product or service will be retained for as long as this data is required.
- Terminated services then follow a deactivation procedure.

Anonymization of personally identifiable information:

- In order to guarantee the privacy of users and to comply with data protection standards, personal data is systematically anonymized before it is stored, insofar as this is possible.
- Anonymization of PII (Personally Identifiable Information) is a measure taken to eliminate potential bias in our machine learning models and ensure that the models work objectively.

14. Security Awareness Service

User data (name, department, e-mail address, group to which user is allocated for analysis purposes) is captured for the Security Awareness Service by means of CSV import, synchronization with MS365 or LDAP synchronization. This data is used to provide awareness training (videos, questionnaires, info sheets) and to send simulated phishing e-mails to the user.

The results of the simulated attacks are analyzed statistically and displayed for each group and each user. Individual-related analysis cannot be carried out if Privacy Mode is enabled. The Employee Security Index (ESI®) is calculated from the gathered information. This illustrates progress in relation to security awareness and allows direct comparisons to be made with a group of very well-trained users.

To ensure that the simulation of phishing scenarios is realistic, fake e-mails are also sent from genuine e-mail addresses at the company. Users can opt out of their e-mail address being used in this way.

To ensure that the simulation of spear phishing e-mails based on OSINT (Open Source Intelligence) is realistic, publicly available company data and personal details are also used, for example information from employer review portals such as Kununu.com or business-related social media sources, for example Xing.com or LinkedIn.com. At higher training levels, fake e-mails can also reference real e-mails previously sent or received, which are completely unrelated to the phishing simulation.

Information entered by users in the context of simulated phishing e-mails, for example login details entered on fabricated login pages that we have set up, is neither processed nor saved. Attachments opened by users in the context of simulated phishing e-mails, for example Word documents or Excel spreadsheets, contain no malicious code.

Processing of reports of potential phishing e-mails in Outlook via the Hornetsecurity addon button:

- If the reported e-mail is a simulated phishing e-mail sent as part of the Security Awareness Service, successful reporting of the e-mail is confirmed to the user and recorded statistically.
- If the e-mail is not a simulated phishing e-mail but the customer is also using the Spam and Malware Filter service, the reported e-mail is sent to our Security Lab for further analysis.

- If the e-mail is not a simulated phishing e-mail and the customer has not ordered the Spam and Malware Filter service, the reported e-mail is sent to a support mailbox of the customer's choosing.

The customer data required for configuring the service and all statistical analyses are deleted no later than 4 weeks after the contract ends.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

15. Spam and Malware Protection

With Spam and Malware Protection, the client's incoming e-mails are filtered for harmful content (e.g. viruses), unwanted advertising (e.g. spam) and legitimate advertising (e.g. newsletters) on the contractor's IT systems. If the client so wishes, outgoing e-mails are also filtered.

Automatic data processing includes the metadata of the message transmission (e-mail address of the sender and recipient, e-mail subject, date/time of e-mail receipt and -delivery, IP addresses of the servers involved in the communication, SMTP error code and text), the content of e-mails and the classification of the e-mail (clean, spam, virus, infomail). The message metadata is used for display in the Control Panel and is deleted after 14 months at the latest. The e-mail itself is deleted after successful delivery or bounce.

Data processing takes place on dedicated hardware, located in leased data centers (colocation).

No other data (e-mail header, sender, addressee, subject, date, text content) will be passed on to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

a. Optional: Advanced Threat Protection (ATP)

ATP protects the client's e-mail traffic against targeted and individual attacks such as spear phishing, blended attacks, advanced persistent threats, ransomware and CEO fraud. In order to detect attacks, the contractor uses advanced filtering techniques to examine e-mails of the client that are classified as suspicious.

For this purpose, meta-information about the e-mail content as well as the e-mail attachment type, -name and -content are processed automatically. The meta-information on the e-mail content is used for display in the control panel and is deleted after 14 months at the latest. The e-mail is deleted from the ATP system after successful analysis.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

b. Optional: Secure Links (as part of ATP)

To enhance security when using our email services, we utilise the 'Secure Links' feature. This involves technically rewriting links contained in incoming emails and, when accessed, checking them first via a security infrastructure.

As part of this check, the destination address and the web content accessible via it are automatically scanned for signs of phishing, malware or other security-related characteristics. Rule-based methods as well as machine learning and deep learning techniques are used for this purpose. Email content is not processed by large language models or generative AI.

The security analysis is limited to the URL accessed and the web resources accessible via it. The content of the email, sender and recipient information, and attachments are not used for the training, fine-tuning or further development of the detection models employed.

Insofar as a URL or the accessed web page itself contains personal data, this may be processed technically as part of the security check. This data is not used for training purposes or to optimise the underlying detection models.

c. Optional: E-mail Encryption

The contractor orders and manages S/MIME certificates, encrypts and signs outgoing e-mails and decrypts incoming e-mails of the client on their own IT systems in accordance with the set guidelines. Depending on the guideline settings, outgoing e-mails are made available to the recipient in the protected Websafe.

The automatic data processing includes the e-mail address of the sender and recipient, the private and public S/MIME or PGP key, the content of outgoing e-mails to third parties (Websafe), the e-mail address in public keys of third parties, the status of the encryption and the content of the e-mail. The sender, recipient and encryption status data are used for display in the Control Panel and are deleted after 14 months at the latest. The e-mail itself is deleted after successful delivery or bounce.

Data processing takes place on dedicated hardware, located in leased data centers (colocation).

To order S/MIME certificates, the e-mail address and first and last name of the certificate applicant are transmitted to a subcontractor in the EU for processing (InterNetX GmbH, Johanna-Dachs-Str. 55, 93055 Regensburg, Germany).

For two-factor authentication (2FA) of the Websafe recipient, the recipient's cell phone number is transmitted to a subcontractor for processing (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA) if consent is given. The transmission takes place on the basis of standard contractual clauses. There, the cell phone number is deleted immediately after the process is completed at Twilio. The contractor stores the cell phone number as long as the recipient's mailbox exists.

No data other than the data specified for the S/MIME certificate order and generation of a 2FA key is passed on to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

d. Optional: Archiving

The contractor archives the client's e-mails in a tamper-proof manner on its own IT systems.

The automatic data processing includes the e-mail address of the sender and recipient, e-mail subject, date/time of e-mail receipt, IP addresses of the servers involved in the communication, the content of e-mails and, if applicable, the name and type of attachment.

The data of the sender and recipient address, e-mail subject, date/time, attachment name and type are used for display in the Control Panel. All this data, including the message itself, is stored for a customer-specific archive period plus 1 year and then deleted. A deletion suspension at the customer's request can increase the storage period.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

e. Optional: Continuity Service

The contractor provides incoming and outgoing e-mails of the client in the archive for a period of 3 months, provided that these e-mails are routed via Hornetsecurity's servers.

The Contractor also provides each user with an e-mail mailbox with 10 GB of storage. Authorized users can access e-mails in this mailbox via a webmail interface or via IMAP and POP3.

Automatic data processing includes message metadata (the e-mail address of the sender and recipient, date/time of e-mail receipt), e-mail content and webmail metadata (login name, IP address, connection duration, retrieval volume, protocol). Message metadata, webmail metadata and archived messages are deleted after 14 months at the latest. Messages in the webmail mailbox are deleted at the latest when the customer no longer uses the service.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

f. Optional: E-mail Signature and Disclaimer

The use of Signature and Disclaimer requires the use of a directory service on the part of the client, which can be queried by the contractor via the LDAP protocol. In addition, the groups from the user directory must be organized in the Control Panel. The messages must be sent via the contractor's relays.

Automatic data processing includes the user's e-mail address, assigned group name in the directory service and any other information linked in the directory service such as organizational affiliation, position, telephone number, fax number and e-mail footer content assigned to the group in the directory on the client's side. The personal data extracted from the directory will be deleted after the end of the use of the service. The processed message is deleted after successful delivery or bounce.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

g. Optional: E-Mail made in Germany

The contractor enables the client's e-mail infrastructure to be connected to the E-Mail made in Germany (EmiG) network and carries out the e-mail server-side implementation needed to meet the requirements for end-to-end transport encryption of e-mails in the EmiG network.

Automatic data processing includes the metadata of the message transmission (e-mail address of the sender and recipient, e-mail subject, date/time of incoming mail, IP addresses of the servers involved in the communication, encryption status) and the content of e-mails. The message transmission metadata is used for display in the Control Panel and is deleted after 14 months at the latest. The e-mail itself is deleted after successful delivery or bounce.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

16. Test Onboarding

To test the performance of the services, you can register directly via our website. For this we need certain information about you personally, the domain, server and user for which the service is required, as well as the desired service. The mandatory fields are marked accordingly. All other information is provided voluntarily. The storage period is therefore generally based on the duration of the contractual relationship. However, alternative legal bases, such as statutory retention periods, may apply after the end of this period.

The client's master data is processed for the purpose of customer master data management by subcontractors on systems in a third country (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). The data is transmitted on the basis of standard contractual clauses.

In this respect, the legal basis for the processing is the implementation of pre-contractual measures or the necessity for the fulfillment of the contract.

17. VM Backup

VM Backup is a reliable, intuitive and easy-to-manage backup and recovery solution for virtualized servers in Hyper-V and VMware environments as well as physical Microsoft servers.

VM Backup enables the customer to perform backups to the locations specified by the customer at the time intervals specified by the customer. The encryption of the backups is ensured by AES-256 encryption keys (password) configured by the customer. All offsite copies are AES-256 encrypted. Encryption is optional for on-site backups (primary) and is also supported.

For offsite copies, data is optionally stored on cloud storage rented by the customer from third-party providers (Microsoft Azure Blob Storage, Wasabi Cloud Object Storage, Amazon S3 or BackBlaze Cloud Storage). The customer acts as the client vis-à-vis those third-party providers.

During operation, the software license used is compared online with the purchased license stored in the master data. The contractor does not transfer or process the usage data of the services.

18. Web Filter

Outgoing http/https and ftp calls from the client are routed via the contractor's proxy server. Data traffic is checked for potentially harmful content and filtered out if necessary.

Automatic data processing includes the date and time a web address was called up, calling IP address, URL called up, classified category of the object called up, authenticated entity: either e-mail address, possibly pseudonymized, or IP address or directory service name and object path or web filter connector string (sAM AccountName, domain ID, computer name, computer IP, calling program). This data (URL without path) is used for display in the Control Panel and is deleted after 14 months at the latest.

Data processing takes place on dedicated hardware, located in leased data centers (colocation). The data is not disclosed to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

The legal basis for the processing of this information and stored data is the necessity for fulfilling the existing contractual relationship.

19. Websafe, privacy policy for third parties

In order for us to provide you with this service, it is necessary to process certain data. The processing of this information and stored data is necessary for the fulfillment of the existing contractual relationship with our customers. This forms the legal basis for processing. When using the Websafe service, you are not subject to automated decision-making as defined by Art. 22 GDPR.

The automatic data processing includes metadata of the message (the e-mail address of the sender and recipient, date/time of e-mail receipt), e-mail content, Websafe metadata (login name, your IP address, connection duration, retrieval volume, protocol) and, if applicable, the number of your mobile device. Your e-mails are stored in Websafe for 3 months. After that they are deleted. Your Websafe account exists as long as you receive e-mails there. If you no longer receive e-mails, your Websafe account will be automatically deleted 12 months after you last received an e-mail. All your personal data and in particular your telephone number are removed from our servers.

To complete your registration, we need to send a PIN to your mobile device. Alternatively, you can contact the sender of your e-mail so that they can forward the PIN to you in another way. The Websafe service provider does not charge any fees for using the Websafe service and sending SMS messages.

The subcontractor for sending the SMS to your mobile device is Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA. The mobile phone number is transmitted on the basis of EU standard contractual clauses. The mobile phone number will be deleted immediately after it is used by Twilio.

The data processing of message metadata, Websafe metadata and messages in the Websafe mailbox takes place on our own hardware, which is located in leased data centers (colocation). The data is not disclosed to third parties. Apart from Hornetsecurity GmbH, no third parties have access to this data.

IV. Right of objection and removal

Where data processing is based on your consent or our legitimate interest, you have the right, at all times, to object to such processing or to withdraw your consent. Your objection or revocation is only effective for the future. You can send an e-mail to datenschutz@hornetsecurity.com at any time in order to exercise your right of objection or revocation. If you object to a processing activity performed on the basis of our legitimate interest, we may continue to perform this activity if we can prove that there are compelling legitimate grounds for such action that outweigh your interests, rights, and freedoms.

V. Rights of data subjects

If data concerning your person is processed, you are considered a data subject as defined by Art. 4 (1) GDPR. As a data subject, you have the following rights in relation to your personal data. In order to exercise these rights, you can contact us using the aforementioned contact details.

a. Right of access according to Art. 15 GDPR

You have the right to information about the personal data concerning you that we process. This includes the mandatory information set forth in Art. 15 GDPR.

b. Right to rectification according to Art. 16 GDPR

You have the right to request that incorrect personal data be immediately rectified and inaccurate personal data be completed.

c. Right of erasure according to Art. 17 GDPR

You have the right to request that your personal data be deleted if one of the reasons specified in Art. 17 GDPR applies, in particular if the legal basis for processing no longer applies.

d. Right to restriction of processing according to Art. 18 GDPR

You have the right to request that the processing of your personal data be restricted if one of the reasons specified in Art. 18 GDPR applies, in particular if this is deemed preferable to the deletion of such data.

e. Right to data portability according to Art. 20 GDPR

You have the right to receive the personal data concerning you in a structured, commonly used, and machine-readable format; you also have the right to transmit said data to another controller without hindrance from the controller to which the personal data has been provided.

f. Right to file a complaint with the competent supervisory authority, Art. 77 GDPR

In accordance with Art. 77 GDPR, you have the right to file a complaint with the competent supervisory authority.

VI. Recipients of data

The processing of your personal data within the scope of the *services* is also partly carried out by processors. Processors are involved exclusively on the basis of an agreement on order processing in accordance with Art. 28 (3) GDPR.

VII. Data transfer to third countries

The personal data that we collect from you in the course of providing the *services* will not be transferred to third countries outside the European Economic Area.

To send text messages with two-factor authentication, we use the provider Twilio, which is based in the USA and therefore in a third country as defined by Art. 44 GDPR. Twilio participates in the EU-U.S. DPF (Data Privacy Framework) and works according to standard contractual clauses, which ensures an adequate level of data protection.

To manage your contract data, we use the provider Salesforce, which is based in the USA and therefore in a third country as defined by Art. 44 GDPR. Salesforce participates in the EU-U.S. DPF (Data Privacy Framework) and works according to certified standard contractual clauses, which ensures an appropriate level of data protection.

To manage your electronic signature for contracts, we use the provider Docusign, which is based in the USA and therefore in a third country in accordance with Art. 44 GDPR. Docusign works according to certified standard contractual clauses, which guarantees an appropriate level of data protection.