Data Privacy Information

Managed Security Services

Hornetsecurity Group

Data Privacy Information

for the Services

- 365 Total Protection (page 5)
- Spam and Malware Protection (page 6), which covers the following products or *Service*s:
  - Hornetsecurity Advanced Threat Protection,
  - Hornetsecurity Email Encryption,
  - Hornetsecurity Archiving,
  - Hornetsecurity Continuity Service,
  - Hornetsecurity Signature and Disclaimer,
  - Hornetsecurity Managed Internet Security SME Service,
  - Email made in Germany,
- Hornetsecurity Hosted Exchange (page 9)
- Web filter (page 9)
- Hornetsecurity Altaro VM Backup (page 10)
- Hornetsecurity Altaro 365 Total Backup (page 10)
- Hornetdrive (page 11)
- Control Panel und Webmail (page 11)
- Test-Onboarding (page 11)

(hereinafter "*Services*", "our *Services*" or "the *Services*").

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

- when or in which circumstances we process data,
- what type of data we process and for what reasons,
- who receives data,
- what rights you have related to our data processing.

This data protection information only refers to the use of personal data within the *Services*. You can download this data protection notice permanently and at any time at the address

https://www.hornetsecurity.com/service-privacy-statement/

I. Contact information

The controller for data processing within the context of the *Services* in terms of the General Data Protection Regulation (GDPR) is always the Customer. Hornetsecurity is acting as a Data Processor in the sense of Art. 28 GDPR. The provision of the *Services* is partly also provided by other Hornetsecurity Group companies as Subcontractors:

	Data Processor	The *Service* is provided in an internal subcontracting relationship through
☐	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Deutschland Telefon: +49 511 515 464-0 E-Mail: info@hornetsecurity.com	-/-
☐	Hornetsecurity Iberia S.L Calle Arte 15, 1ª 28033, Madrid España Teléfono: +34 91 368 77 33 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Aegis Security Argentina S.A. Belgrano 53 Piso, PB Dpto: B Tandil, Buenos Aires Argentina Tel: +54 9 249 449 9296 E-mail: info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☒	Hornetsecurity Ltd. 55 Baker Street London, W1U7EU United Kingdom Fon: +44 203 0869 833 Email: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 United States Fon: +1 (412) 924-5300 E-mail: sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com

We have also appointed a data protection officer. You can contact said officer at: privacy@hornetsecurity.com.

II. General data processing information

1. Scope of processing of personal data

Providing the *Service*s requires the processing of different types of data. The scope of data processing also depends on your use of the functionalities provided by the *Service*s – for example, what type of data you process or have processed there, or your consent to the processing of data.

As part of the agreement concluded with Hornetsecurity about the use of the *Service*s, you are obliged to provide the personal data required to fulfill the agreement. The refusal to provide this information may constitute a breach of duty which could result in your having to pay damages. You are not obliged to provide us with any personal data. If, however, the provision of such data is technically necessary to use our *Service*s, a refusal will result in your not being able to use our *Service*s.

When using the *Service*s you are not subject to any automated decision-making within the meaning of Article 22 GDPR.

2. Legal basis for processing personal data

The legal basis for processing personal data is presented below.

Processing basis	Legal basis in the GDPR	Explanation
Fulfillment of agreement or execution of pre-contractual measures	Article 6 para. 1 b)	Data is processed only to the extent necessary for the performance and fulfillment of the rights and obligations under the agreement. Unless expressly stated otherwise, we process data solely within this scope.
Legitimate interest	Article 6 para. 1 f)	We process data if we have a legitimate interest in doing so and if no predominant opposing interests of the data subject are evident. The specific interest is explained within this Data Privacy Information in the description of the processing.
Legal duty	Article 6 para. 1 c)	We process data only if processing is necessary to fulfill German or European legal obligations.

III. Data processing for operating the *Services*

In order for us to be able to provide you with the *Service*s, we need to process certain data.

The legal basis for processing this information and the stored data is the need to fulfill the existing contractual relationship. The storage period is based on the duration of the contractual relationship. However, once it expires, an alternative legal basis – such as statutory retention periods – may apply.

1. Basic data

The entity responsible for processing the master and configuration data is the entity from the Hornetsecurity Group, which is identified as the Data Processor under I, "Contact details".

1.1. Master data

The customer's master data (name, address, contact person, telephone number, email address, department, position, booked *Service*s, billing period, account details) are recorded for purposes of managing and fulfilling the contractually agreed *Service*s. Personal data of co-users (email addresses) are recorded and used for purposes of fulfilling the agreed *Service*s.

The processing of co-user data is performed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

To maintain the client base, the customer's master data is transferred to and processed by a subcontractor on systems in a third country (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). This data transfer is based on Standard Contractual Clauses.

Furthermore, parts of the Contractor's client base are shared with subcontractors within the EU (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Germany) and processed on their systems for purposes of invoicing and billing (by letter or email).

1.2. Configuration data

The technical configuration of the booked *Service* is saved in connection with the user's email address, corresponding affiliation to a user group, or the customer's domain name.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

For Hornetsecurity Altaro VM Backup and Hornetsecurity Altaro 365 Total Backup also applies:

For validation of the license, the master data (email address) required for unique identification is transferred to the systems of Altaro Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malta, EU.

2. 365 Total Protection

The Spam and Malware Protection checks the customer's incoming emails and filters them on the contractor's IT systems for harmful content (e.g. viruses), unsolicited advertising (e.g. spam) and legitimate advertising (e.g. newsletters). Outgoing emails are also filtered.

Automatic data processing includes metadata on email delivery (sender and recipient email address, email subject, date/time of incoming and outgoing email, IP addresses of the servers involved in the communication, SMTP error code and text), email content, and email classification (clean, spam, virus, info mail). The metadata on the email content are used for display in the control panel and deleted after a maximum storage period of 14 months. The email itself is deleted after successful delivery or bounce.

The use of user-based individual signatures/company disclaimer/1-click intelligent ads requires the use of a directory service on the part of the customer, which can be queried by the contractor via the LDAP protocol. In addition, the groups in the user directory must be organized in the control panel. The emails must be sent via the contractor's relays.

The automatic data processing includes the email address of the user, assigned group name in the directory service, further information that may be linked in the directory service, e.g., organizational affiliation, position, phone number, fax number, and mail footer contents, which are assigned to the customer's group in the directory. Personal data obtained from the directory shall be deleted after the service has been used. The processed email is deleted after successful delivery or bounce.

Global S/MIME & PGP encryption: The contractor encrypts and signs outgoing emails as well as encrypts the customer's incoming emails on its own IT systems in accordance with the set guidelines. Depending on the rule setting, outgoing emails are delivered to the recipient in the secure WebSafe.

Automatic data processing includes sender and recipient email address, private and public S/MIME or PGP key, outgoing email content to third parties (Websafe), mail address in third party public keys, status of encryption and content of emails. The information about the sender, recipient, and encryption status is used for display in the control panel and deleted after a maximum storage period of 14 months. The email itself is deleted after successful delivery or bounce.

Email archive: The contractor archives customer emails securely on its own IT systems in an audit-proof fashion.

The automatic data processing includes sender and recipient email address, email subject, date/time of the incoming email, IP addresses of the servers involved in the communication, as well as the name and type of attachment, if applicable.

The information about the sender and recipient address, email subject, date/time, as well as the name and type of attachment, is used for display in the control panel. All these data, incl. the message itself, are archived for a customer-specific duration plus one year and then deleted. The storage duration can be extended on customer request.

Advanced Thread Protection (ATP): protects the client's email traffic from targeted and individual attacks, such as spear phishing, blended attacks, advanced persistent threats, ransomware, and CEO fraud. To detect attacks, customer emails that are classified as suspicious are examined using advanced filtering techniques.

This entails automatic processing of the metadata on the email content and type, name, and content of attached files. The metadata on the email content are used for display in the control panel and deleted after a maximum storage period of 14 months. The email is deleted from the ATP system after successful analysis.

Contingency covering: The Contractor shall provide an email mailbox with 10 GB of storage space per user in the event of a failure of the target server. Emails in this mailbox can be accessed by authorized users through a webmail interface or via IMAP and POP3.

The automatic data processing includes email metadata (sender and recipient email address, date/time of incoming email), email content, as well as webmail metadata (login name, IP address, connection duration, volume of downloaded content, and protocol). Email metadata, webmail metadata, and archived messages are deleted after a maximum storage duration of 14 months. At the latest, the messages in the webmail inbox are deleted when the customer no longer uses the service.

The data are processed on owned hardware placed in the rented data centers (colocation).

For the use of single-sign-on, the email address is passed on to Microsoft when the user registers.

No other data will be passed on to third parties, nor will third parties have access to the data.

The legal basis for processing this information and the stored data is the need to fulfill the existing contractual relationship.

3. Spam and Malware Protection

This checks the customer's incoming emails and filters it on the Contractor's IT systems for harmful content (e.g. viruses), unsolicited advertising (e.g. spam) and legitimate advertising (e.g. newsletters). Outgoing emails can also be filtered, if desired by the customer.

The automatic data processing includes metadata on email delivery (sender and recipient email address, email subject, date/time of incoming and outgoing email, IP addresses of the servers involved in the communication, SMTP error code and text), email content, and email classification (clean, spam, virus, info mail). The metadata on the email content are used for display in the control panel and deleted after a maximum storage period of 14 months. The email itself is deleted after successful delivery or bounce.

The data is processed on owned hardware placed in the rented data centers (colocation).

The transmission of other data (mail header, sender, recipient, subject, date, mail text) to third parties does not take place. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.1. Optional: Advanced Threat Protection (ATP)

ATP protects the customer's email traffic against targeted and individual attacks such as spear phishing, blended attacks, advanced persistent threats, ransomware, and CEO fraud. To detect attacks, customer emails that are classified as suspicious are examined using advanced filtering techniques.

This entails automatic processing of the metadata on the email content and type, name, and content of attached files. The metadata on the email content are used for display in the control panel and deleted after a maximum storage period of 14 months. The email is deleted from the ATP system after successful analysis.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.2. Optional: Email Encryption

The Contractor orders and manages S/MIME-certificates, encrypts and signs outgoing emails as well as encrypts the customer's incoming emails on its own IT systems in accordance with the set guidelines. Depending on the rule setting, outgoing emails are delivered to the recipient in the secure WebSafe.

The automatic data processing includes the sender and recipient email address, private and public S/MIME or PGP key, outgoing emails to third parties (WebSafe), email address in third-party public keys, encryption status, and content of the emails. The information about the sender, recipient, and encryption status is used for display in the control panel and deleted after a maximum storage period of 14 months. The email itself is deleted after successful delivery or bounce.

The data is processed on owned hardware placed in the rented data centers (colocation).

To order S/MIME certificates, the e-mail address and first and last name of the certificate purchaser are transmitted to a subcontractor in the EU for processing (PSW Group GmbH, Flemingstr. 20-22, 36041 Fulda, Germany).

For a two-factor authentication (2FA) of the Websafe receiver, its mobile phone number is optionally transmitted to a subcontractor for processing. (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA). The transmission takes place on basis of Standard Contractual Clauses.

No data other than that specified for the S/MIME certificate order and generation of a 2FA will be passed on to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.3. Optional: Archiving

The Contractor archives customer emails securely on its own IT systems in an audit-proof fashion.

The automatic data processing includes sender and recipient email address, email subject, date/time of the incoming email, IP addresses of the servers involved in the communication, as well as the name and type of attachment, if applicable.

The information about the sender and recipient address, email subject, date/time, as well as the name and type of attachment, is used for display in the control panel. All these data, incl. the message itself, are archived for a customer-specific duration plus one year and then deleted. The storage duration can be extended on customer request.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.4. Optional: Continuity Service

The Contractor archives the customer's incoming and outgoing emails for three months, provided that those emails are routed through Hornetsecurity servers.

The Contractor also provides each user with a mailbox holding 10 GB of storage space. Emails in this mailbox can be accessed by authorized users through a webmail interface or via IMAP and POP3.

The automatic data processing includes email metadata (sender and recipient email address, date/time of incoming email), email content, as well as webmail metadata (login name, IP address, connection duration, volume of downloaded content, and protocol). Email metadata, webmail metadata, and archived messages are deleted after a maximum storage duration of 14 months. At the latest, the messages in the webmail inbox are deleted when the customer no longer uses the *Service*.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.5. Optional: Email signature and disclaimer

The use of the Signature and Disclaimer requires the customer to have a directory *Service* that can be queried by the Contractor via the LDAP protocol. In addition, the groups in the user directory must be organized in the control panel. The emails must be sent via the Contractor's relays.

The automatic data processing includes the email address of the user, assigned group name in the directory *Service*, further information that may be linked in the directory *Service*, e.g., organizational affiliation, position, phone number, fax number, and mail footer contents, which are assigned to the customer's group in the directory. Personal data obtained from the directory shall be deleted after the *Service* has been used. The processed email is deleted after successful delivery or bounce.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

3.6. Optional: Email made in Germany

The Contractor facilitates connection of the customer's email infrastructure to the Email made in Germany (EmiG) network and ensures appropriate implementation on the mail server to ensure compliance with all requirements for continuous transport encryption of emails in the EmiG network.

The automatic data processing includes the email metadata (sender and recipient email address, email subject, date/time of the incoming email, IP addresses of the servers involved in the communication, encryption status), and email content. The email metadata are used for display in the control panel and deleted after a maximum storage period of 14 months. The email itself is deleted after successful delivery or bounce.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

4. Hosted Exchange

In addition to the Spam and Malware Protection, the customer can also obtain Hosted Exchange mailboxes from the Contractor if no mail server of its own should be used. Hosted Exchange allows you secure operation of professionally managed Exchange Servers in your mail domain with Active Sync, shared contact information, online calendar, group collaboration, and access from multiple clients and hardware platforms.

The automatic data processing includes received and sent emails, email addresses of the user, group memberships, date of creation of the mailbox, access rights from/to other internal accounts on the same domain and mobile devices used to access the mailbox. Furthermore, if filled in: company, position, department, employee number, supervisor, phone numbers, address. The data shall be deleted no later than 90 days after termination of the *Service*.

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

The legal basis for processing this information and the stored data is the need to fulfill the existing contractual relationship.

5. Web filter

Outgoing http/https and ftp calls by the customer are directed via the Contractor's proxy servers. The data traffic is checked for potentially harmful content, which is filtered out if necessary.

The automatic data processing includes the date and time the web address was accessed, the accessing IP address, visited URL, classified category of the accessed object, authenticated entity: either email address, pseudonymized (circumstances permitting), IP address, or directory *Service* name and object path or Web Filter connector string (sAMAccountName, domain ID, computer name, computer IP, accessing program). The aforementioned data (URL without

path) are used for display in the control panel and deleted after a maximum storage period of 14 months.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

The legal basis for processing this information and the stored data is the need to fulfill the existing contractual relationship.

6. Hornetsecurity Altaro VM Backup

Hornetsecurity Altaro 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.

Hornetsecurity Altaro VM Backup allows customers to perform backups to customer-specified locations at customer-specified time intervals. Encryption of backups is ensured by customer-configured AES-256 encryption keys (password). All offsite copies are AES-256 encrypted. For onsite (primary) backups, encryption is optional 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 or Wasabi Cloud Object Storage or Amazon S3). The customer acts as the Data Controller in relation to the third-party providers.

During operation, the software license used is matched online with the purchased license stored in the master data. A transfer to or processing of the user data of the *Services* by the contractor does not take place.

7. Hornetsecurity Altaro 365 Total Backup

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

Hornetsecurity Altaro 365 Total Backup offers customers a policy-based configuration, overview and monitoring of permissions, backups and MS365 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 performed within the Hornetsecurity Group by Altaro Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malta ("Altaro"). Altaro's storage of encrypted backup data is located in the Microsoft Azure Cloud, Western Europe Zone, where Altaro uses 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 matched online with the purchased license stored in the master data. A transfer to or processing of the user data of the *Services* by the contractor does not take place.

8. Hornetdrive

Hornetdrive enables safe storage, sharing, and joint editing of files in the cloud.

The automatic data processing includes the registered email address, date of the initial setup, name of the devices used, date of the first and last access from this device, operating system version of the device, drive name of the created drive and creation date, used drive volume, and total occupied disk space.

The data is processed on owned hardware placed in the rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the customer, no third parties have access to the data.

The legal basis for processing this information and the stored data is the need to fulfill the existing contractual relationship.

9. Registration via the control panel and webmail

If you are already a Hornetsecurity customer, you can register via our website in the Control Panel from which you can use and manage your *Service*s. As a webmail customer, you can register via a separate link in your mailbox. To register, you will need your username and/or e-mail address as well as your password. The storage period is based on the length of the contractual relationship. Once it expires, however, an alternative legal basis – such as statutory retention periods – may apply.

The data processing is performed on own hardware, which is located in rented data centers (colocation). The data are not transferred to third parties. Besides the Contractor and the named representatives of the client, no third parties have access to the data.

The legal basis for processing this information and all the data stored in Hornetsecurity's *Service*s is the need to fulfill the existing contractual relationship.

10. Test onboarding

In order to test the performance of the *Services*, you may register directly via our website. For this purpose, we require various information about you personally, the domain, server and user for which the service is desired, as well as the desired service. The mandatory fields are marked accordingly. All other information is provided voluntarily. The duration of storage is determined by the duration of the contractual relationship. After the end of the contractual relationship, however, alternative legal bases may apply, such as statutory storage periods.

The data processing of the customer's master data is transferred to subcontractors on systems in a third country (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA) for the purpose of customer master data maintenance. The transfer of data takes place based on standard contractual clauses.

The legal basis for the processing is the implementation of pre-contractual measures or the necessity for the fulfillment of the contract.

IV. Recipients of data

The processing of your personal data within the scope of the Services is partly also carried out by processors. These are only included on the basis of a commissioned processing agreement in accordance with Art. 28 para. 3 GDPR.

V. Data transmission to third countries

The personal data we collect from you in the context of the Services will not be transferred to third countries outside the European Economic Area.

For the management of your contract data, we use the provider Salesforce based in the USA and thus in a third country in accordance with Art. 44 GDPR. Salesforce is certified according to standard contractual clauses.

VI. Possibility of objection and removal

Insofar as the data processing is based on your consent or our legitimate interest, you have the right to object to the processing at any time or to revoke your consent. Your objection or revocation only has effect for the future. You can contact privacy@hornetsecurity.com to exercise your right of objection or withdrawal at any time. If you are object to processing on the basis of our legitimate interest, we may nevertheless continue the processing if we can prove compelling legitimate grounds for the processing that outweigh your interests, rights and freedoms.

VII. Data subject rights

If data related to your person is processed, you are a data subject within the meaning of Art. 4 (1) GDPR. As a data subject, you have the following rights in regards to your personal data. To exercise these rights, you can contact us using the contact details above.

Right to gain access pursuant to Art. 15 GDPR

You have a right to information about your personal data processed by us. This includes the mandatory information presented in Art. 15 GDPR.

Right to correction pursuant to Art. 16 GDPR

You have the right to request the immediate rectification of incorrect personal data as well as the completion of incorrect personal data.

Right to erasure pursuant to Art. 17 GDPR

You have the right to request the deletion of your personal data if one of the reasons referred to in Art. 17 GDPR intervenes, in particular if there is no longer a legal basis for the processing.

Right to restriction of processing according to Art. 18 GDPR

You have the right to request the restriction of the processing of your personal data if one of the reasons referred to in Art. 18 GDPR intervenes, in particular at your request instead of erasing the data.

Right to data portability according to Art. 20 GDPR

You have the right to request all personal data stored by us about you in a structured, commonly used and machine-readable format and to transmit this data to another controller without hindrance by the controller to whom the personal data was provided.

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

In accordance with Art. 77 GDPR, you have the right to lodge a complaint with the supervisory authority responsible for you.