Data Privacy Policy

Managed Security Services

Hornetsecurity Group

Data Privacy Policy

For "the services"

- Threat Monitor

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 Hornetsecurity products Threat Monitor.
You can download this data protection notice permanently and at any time at address https://www.hornetsecurity.com/service-privacy-statement/

I. Contact information

The controller for data processing within the context of the Hornetsecurity products Threat Monitor 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 services is partly also provided by other Hornetsecurity group companies as subcontractors:

	Data Processor	The service is provided in an internal sub-contracting 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: info@spamina.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: ruben.mansilla@spamina.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Fon: +49 511 515 464-0 E-mail: info@hornetsecurity.com
☐	Hornetsecurity Limited 150 Aldersgate Street, London, EC1A 4AB United Kingdom Fon: +44 2030 869833 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 Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 United States Fon: +1 (412) 924-5300 E-mail: info@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 Spam and Malware Protection, web filter and Hornetdrive services requires the processing of different types of data. The scope of data processing also depends on your use of the functionalities provided by the services – 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 services, 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 services, a refusal will result in your not being able to use our services.

When using the services Spam and Malware Protection, web filter and Hornetdrive services 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 Threat Monitor

In order for us to be able to provide you with the services, 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

1.1. Master data

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

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.

The communication data of the administrative contacts designated by the customer are compared with the official contact options stored in the directory service, so that Hornetsecurity can guarantee a quick telephone contact with these persons in the event of a recognised high risk.

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 Binding Corporate Rules.

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.

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

2. Threat Monitor, Test Onboarding

When using the Threat Monitor, incoming emails from the customer are checked for harmful content (e.g. viruses), unwanted advertising (e.g. spam) and legitimate advertising (e.g. newsletters). This is carried out in the form of a temporary copy of the emails on the IT systems of the contractor.

Automatic data processing includes the administrative email address for Azure services, message delivery metadata (mail address of the sender and recipient, mail subject, date/time of mail receipt and mail delivery to the recipient server, IP addresses of the servers involved in the communication), the email body (actual content of the email) and the classification of the email (clean, spam, threat, infomail). The message metadata is used for display in the Control Panel and Threat Monitor app, and to identify the email in the recipient's mailbox.

Metadata is deleted from the contractor's systems after 14 months at the latest. The email body is deleted from the contractor's systems immediately after classification.

Data processing is carried out on the contractor's own hardware, which is located in rented data centers (colocation).

Email body or email metadata will not be passed on to third parties. Apart from the contractor and designated representatives of the client, no third parties have access to the data.

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

IV. Data transmission to third countries

The personal data that we collect from you as part of our Threat Monitor services shall not be transmitted to third countries outside the European Economic Area.

To manage your contract data, we commission the services of Salesforce, based in the US and thus, pursuant to Art. 44 GDPR, in a third country. Salesforce has established officially verified Standard Contractual Clauses and therefore ensures an appropriate level of data protection.

To manage your electronic signature on contracts, we commission the services of Docusign, based in the US and thus, pursuant to Art. 44 GDPR, in a third country. Docusign has established officially verified Standard Contractual Clauses and therefore ensures an appropriate level of data protection.