Información sobre la protección de datos

Managed Security Services

Hornetsecurity Group

Información sobre la protección de datos

Para "los servicios"

- Spam and Malware Protection, el cual comprende los siguientes productos o servicios:
  - Advanced Threat Protection de Hornetsecurity
  - Email Encryption de Hornetsecurity
  - Archiving de Hornetsecurity
  - Continuity Service de Hornetsecurity
  - Signature and Disclaimer de Hornetsecurity
  - E-Mail made in Germany
- Hosted Exchange de Hornetsecurity
- Web Filter
- Hornetdrive
- Control Panel y Webmail

La base de una protección de datos eficaz es una información completa sobre la recogida, el tratamiento y el uso de sus datos ("tratamiento de datos"). Por tanto, desearíamos informarle sobre los siguientes aspectos:

- Cuándo o durante qué acciones tratamos los datos
- Qué datos tratamos y por qué motivos
- Quién recibe los datos
- Qué derechos le corresponden debido al tratamiento de datos por nuestra parte

La presente información sobre la protección de datos solo se refiere al uso de datos personales en el marco de los productos de Hornetsecurity: Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail.
Puede acceder a esta información sobre la protección de datos, imprimirla o descargarla de forma permanente y en cualquier momento a través del enlace:
https://www.hornetsecurity.com/service-privacy-statement/

I. Datos de contacto

El responsable del tratamiento de los datos en relación a los productos de Hornetsecurity Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail en el sentido del Reglamento General de Protección de Datos (RGPD) siempre es el cliente. Hornetsecurity actúa como encargado del tratamiento según el artículo 28 del RGPD. La prestación de servicios también será realizada en parte por otras empresas del grupo Hornetsecurity actuando como subcontratistas

	Encargado del tratamiento	El prestador del servicio, en una relación de subcontratación interna, es
☐	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Alemania Teléfono: +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 Alemania Teléfono: +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 Estados Unidos Teléfono: +1 (412) 924-5300 E-mail: info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177 Hannover Germany Teléfono: +49 511 515 464-0 E-mail: info@hornetsecurity.com

También hemos nombrado a un delegado de protección de datos. Sus datos de contacto son: privacy@hornetsecurity.com.

II. Información general sobre el tratamiento de datos

1. Alcance del tratamiento de los datos personales

La prestación de los servicios Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail requiere el tratamiento de diferentes datos. Además, el alcance del tratamiento de datos depende del uso que usted haga de las funcionalidades de los servicios (por ejemplo, qué datos trate o haga tratar usted, o consienta que se traten).

En el marco del contrato celebrado con Hornetsecurity sobre el uso de los servicios, usted está obligado a proporcionar los datos personales necesarios para la ejecución del contrato. Su negativa a proporcionar estos datos puede constituir un incumplimiento de obligaciones que podría obligarlo al pago de indemnización por daños y perjuicios. Usted no está obligado a proporcionarnos datos personales. Sin embargo, en la medida en que la comunicación de dichos datos esté técnicamente relacionada con el uso de nuestros servicios, la negativa a comunicarlos provocará que usted no pueda utilizar nuestros servicios.

Cuando utilice los servicios Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail, no será objeto de una decisión automatizada en el sentido del artículo 22 del RGPD.

2. Fundamento jurídico del tratamiento de datos personales

A continuación se exponen los fundamentos jurídicos del tratamiento de datos personales.

Razón del tratamiento	Fundamento jurídico del RGPD	Explicación
Ejecución del contrato o ejecución de medidas precontractuales	Art. 6, apartado 1 b)	El tratamiento solo se llevará a cabo en la medida necesaria para el ejercicio y la ejecución de los derechos y obligaciones derivados del contrato. Salvo indicación expresa de lo contrario, el tratamiento de datos por nuestra parte solo se efectuará en el volumen indicado.
Interés legítimo	Art. 6, apartado 1, letra f)	El tratamiento se efectuará siempre que tengamos un interés legitimo para ello y no prevalezcan intereses del interesado en el sentido contrario. El interés concreto se explica en esta declaración de protección de datos en el contexto de la descripción del tratamiento.
Obligación legal	Art. 6, apartado 1, letra c)	Se efectuará un tratamiento en la medida en que esto sea necesario para el cumplimiento de obligaciones legales alemanas o europeas.

III. Tratamiento de datos para la prestación de los servicios Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail

Para que podamos proporcionarle los servicios, es necesario tratar ciertos datos. El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente. Por tanto, el período de almacenamiento dependerá principalmente de la duración de la relación contractual. Sin embargo, una vez finalizada la misma, pueden ser de aplicación fundamentos jurídicos alternativos, tales como la existencia de plazos legales de almacenamiento.

1. Datos básicos

1.1. Datos maestros

Los datos maestros del cliente (nombre, dirección, persona de contacto, número de teléfono, dirección de correo electrónico, departamento, cargo, servicios contratados, período de facturación, datos bancarios) se registran para la administración de los servicios y se utilizan para la prestación de los servicios acordados en el contrato. Los datos personales de los cousuarios (dirección de correo electrónico) se recogen y utilizan para la prestación de los servicios acordados en el contrato.

El tratamiento de los datos de los cousuarios se realiza en hardware propio alojado en los centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

Con fines de gestión de la cartera de clientes, los datos maestros del cliente son tratados por un subcontratista en sistemas ubicados en un tercer país (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, EE. UU.). La transferencia de datos se lleva a cabo de conformidad con cláusulas contractuales tipo de la UE.

Aparte de esto, con el fin de la entrega y el envío de facturas (por correo ordinario o electrónico), parte de los datos maestros del cliente se transmiten a subcontratistas dentro de la UE y se tratan en sus sistemas (PIN Mail AG, Alt-Moabit 91, 10559 Berlín, Alemania).

1.2. Datos de configuración

La configuración técnica de cada servicio contratado se almacena en relación con la dirección de correo electrónico del usuario, la pertenencia al grupo de un usuario o el nombre de dominio del cliente.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity se basa en la necesidad de cumplir con la relación contractual existente.

2. Spam and Malware Protection

Spam and Malware Protection filtra los correos electrónicos entrantes del cliente para detectar contenidos dañinos (p. ej., virus), publicidad no deseada (p. ej., spam) y publicidad legítima (p. ej. newsletters) en los sistemas informáticos del contratista. Si el cliente así lo desea, se filtran también los mensajes salientes.

El tratamiento automático de datos incluye metadatos de transmisión de mensajes (direcciones de correo electrónico del remitente y del destinatario, asunto del correo electrónico, fecha y hora de recepción y entrega, direcciones IP de los servidores implicados en la comunicación, código de error SMTP y texto), contenido de los correos electrónicos y clasificación del correo electrónico ("Limpio", "Spam", "Virus", "Infomail"). Los metadatos de los mensajes se utilizan para su visualización en Control Panel y se eliminan, a más tardar, al cabo de 14 meses. El correo en sí se elimina tras su entrega o tras su devolución.

El tratamiento de los datos se efectúa en hardware propio ubicado en centros de datos arrendados (housing).

No se transmite ningún otro dato a terceros (encabezado del correo, remitente, destinatario, asunto, fecha, contenido textual). Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

2.1. Opcional: Advanced Threat Protection (ATP)

ATP protege el tráfico de correo electrónico del cliente frente a ataques dirigidos e individuales, tales como el Spearphishing (suplantación de identidad selectiva), Blended Attacks (ataques combinados), Advanced Persistent Threats (amenazas persistentes avanzadas), Ransomware (software de extorsión) y el fraude del CEO. Para detectar ataques, el contratista utiliza técnicas avanzadas de filtrado para examinar los correos electrónicos del cliente que han sido clasificados como sospechosos.

Para ello, se procesan automáticamente metadatos sobre el contenido del correo, así como sobre el tipo de archivo adjunto, su nombre y su contenido. Los metadatos sobre el contenido del correo se utilizan para su visualización en Control Panel y se eliminan, a más tardar, al cabo de 14 meses. El correo se elimina del sistema ATP tras su correcto análisis.

El tratamiento de los datos se efectúa en hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

2.2. Opcional: Servicio de cifrado de correo electrónico

El contratista solicitará y administrará certificados S/MIME y cifrará y firmará correos electrónicos salientes del cliente en sus propios sistemas informáticos conforme a las directrices establecidas. En función de las directrices establecidas, los correos electrónicos salientes se pondrán a disposición del destinatario en el Websafe, un espacio web protegido.

Los datos tratados de modo automático comprenden la dirección de correo electrónico del remitente y del destinatario, las claves privada y pública S/MIME o PGP, el contenido de correos salientes dirigidos a terceros (Websafe), la dirección de correo electrónico en claves públicas de terceros, el estado del cifrado y el contenido del correo electrónico. Los datos del remitente, del destinatario y del estado del cifrado se utilizan para su visualización en el Control Panel y se borran, a más tardar, al cabo de 14 meses. El correo en sí se elimina tras su entrega o tras su devolución.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing).

Para la solicitud certificados S/MIME, se transmiten la dirección de correo electrónico, el nombre y los apellidos del solicitante del certificado a un subcontratista ubicado en la UE (PSW Group GmbH, Flemingstr. 20-22, 36041 Fulda, Alemania) para su tratamiento.

Opcionalmente, para una autenticación en dos pasos (2FA) del destinatario de Websafe, se transmite su número de teléfono móvil a un subcontratista (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, EE.UU.). La transferencia de los datos se efectúa en conformidad con cláusulas contractuales tipo de la UE.

No se transfieren a terceros otros datos distintos a los mencionados para la solicitud y la generación de una clave para autenticación en dos pasos. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

2.3. Opcional: Archiving

El contratista archiva los correos electrónicos del cliente en sus propios sistemas informáticos de modo apto para auditoría.

Los datos tratados de modo automático comprenden la dirección de correo electrónico del remitente y del destinatario, el asunto del correo, la fecha y la hora de recepción del correo, las direcciones IP de los servidores implicados en la comunicación, el contenido de los correos electrónicos y, de haberlo, el nombre y el tipo de archivo adjunto.

La dirección del remitente y del destinatario, el asunto del correo, la fecha/hora, el nombre del archivo adjunto y el tipo de archivo adjunto se utilizan para su visualización en el Control Panel. Todos estos datos, incluido el mensaje en sí mismo, se almacenan durante el periodo de archivo de específico del cliente más 1 año, a continuación, se borran. El tiempo de almacenamiento puede aumentar si, por deseo del cliente, se establece una prohibición de eliminación de los datos.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

2.4. Opcional: Continuity Service

El contratista proporcionará los correos electrónicos entrantes y salientes del cliente en el archivo durante un período de 3 meses, siempre y cuando dichos correos electrónicos se dirijan a través de los servidores Hornetsecurity.

Además, el contratista proporcionará un buzón de correo electrónico con 10 GB de espacio de almacenamiento por usuario. Los usuarios autorizados pueden acceder a los correos electrónicos de este buzón a través de una interfaz web de correo electrónico o mediante IMAP y POP3.

Los datos tratados de modo automático comprenden metadatos de mensajes (dirección de correo electrónico del remitente y del destinatario, fecha y hora de recepción del correo), contenido del correo y metadatos de webmail (nombre de inicio de sesión, dirección IP, duración de la conexión, volumen de acceso, protocolo). Los metadatos de mensajes, los metadatos de correo web y los mensajes archivados se eliminan, a más tardar, al cabo de 14 meses. Los mensajes contenidos en el buzón de correo web se eliminan, a más tardar, cuando el cliente deja de utilizar el servicio.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

2.5. Opcional: Signature and Disclaimer

La utilización del servicio Signature and Disclaimer requiere el uso, por parte del cliente, de un servicio de directorio que el contratista pueda consultar a través del protocolo LDAP. Además, los grupos del directorio de usuarios deben estar organizados en el Control Panel. Los mensajes deben enviarse a través de los relays del contratista.

Los datos tratados de modo automático comprenden la dirección de correo electrónico del usuario, el nombre del grupo asignado en el servicio de directorio y otros datos que puedan estar vinculados al servicio de directorio, tales como la organización a la que pertenezca el usuario, su cargo, número de teléfono, número de fax y el contenido del pie de página del correo que el cliente asigna al grupo en el directorio. Los datos personales recogidos del directorio se borrarán una vez finalizada la utilización del servicio. El mensaje procesado se borra después de su entrega o devolución.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

2.6. Opcional: E-Mail made in Germany

El contratista posibilita la conexión de la infraestructura de correo electrónico del cliente a la red E-Mail made in Germany (EmiG) y, para ello, efectúa la implementación necesaria en el servidor de correo para cumplir con los requisitos de cifrado de transferencia continua de correos electrónicos en la red EmiG.

Los datos tratados de modo automático comprenden los metadatos de la transmisión de mensajes (dirección de correo electrónico del remitente y del destinatario, asunto del correo electrónico, fecha/hora de recepción del correo, direcciones IP de los servidores implicados en la comunicación, estado del cifrado) y el contenido de los correos electrónicos. Los metadatos de la transmisión de mensajes se utilizan para su visualización en el Control Panel y se borran, a más tardar, al cabo de 14 meses. El correo en sí se elimina tras su entrega o tras su devolución.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

3. Hosted Exchange

Junto con Spam and Malware Protection, el cliente puede adquirir buzones de Hosted Exchange si no va a utilizar un servidor de correo propio. Hosted Exchange le permite emplear, de modo seguro y sin esfuerzo adicional, un servidor Exchange gestionado profesionalmente en su dominio de correo con Active Sync, información de contacto compartida, calendario en línea, colaboración en grupo y acceso desde múltiples clientes y plataformas de hardware.

Los datos tratados de modo automático comprenden los correos electrónicos recibidos y enviados, la dirección de correo electrónico del usuario, pertenencias a grupos, la fecha de creación del buzón de correo, permisos de/sobre otras cuentas internas en el mismo dominio y dispositivos móviles utilizados para acceder al buzón de correo. También, si se comunican tales datos, se incluyen la empresa, el cargo, el departamento, el número de empleado, el supervisor, los números de teléfono y la dirección. Los datos se borrarán en un plazo máximo de 90 días tras la finalización del servicio.

Los correos electrónicos se transmiten a servidores de subcontratistas ubicados en la UE para su tratamiento y conservación (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Alemania o Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Alemania).

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

4. Web Filter

Las solicitudes http/https y ftp salientes del cliente se dirigen a través del servidor proxy del contratista. El tráfico de datos se comprueba en busca de contenido potencialmente dañino y, si es preciso, se filtra.

Los datos tratados de modo automático comprenden la fecha y la hora del solicitud de una dirección web, la dirección IP solicitada, la URL solicitada, la categoría clasificada del objeto solicitado y la entidad autenticada: o bien la dirección de correo electrónico, posiblemente bajo pseudónimo, o bien la dirección IP, o bien el nombre del servicio de directorio y la ruta del objeto, o bien la cadena del conector de Web Filter (sAMAccountName, ID de dominio, nombre del ordenador, IP del ordenador, programa de acceso). Los datos mencionados (URL sin ruta) se utilizarán para su visualización en el Control Panel y se borrarán, a más tardar, al cabo de 14 meses.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

5. Hornetdrive

Hornetdrive permite almacenar, intercambiar y editar en común archivos ubicados en la nube de modo cifrado.

Los datos tratados de modo automático comprenden la dirección de correo electrónico registrada, la fecha de la configuración inicial, el nombre de los dispositivos utilizados, la fecha del primer y último acceso desde este dispositivo, la versión del sistema operativo del dispositivo, los nombres de las unidades de disco creadas y la fecha de creación, el volumen de almacenamiento utilizado, la suma del espacio en disco ocupado y los contenidos de los archivos cifrados del usuario.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

6. Inicio de sesión en Control Panel y Webmail

Si ya es cliente de Hornetsecurity, puede iniciar sesión en el Control Panel de nuestro sitio web, desde donde podrá utilizar y gestionar sus servicios. Como cliente de correo web, puede iniciar sesión en su buzón de correo electrónico a través de un enlace por separado. Para iniciar sesión necesitará su nombre de usuario o dirección de correo electrónico y su contraseña. Por tanto, el período de almacenamiento dependerá principalmente de la duración de la relación contractual. Sin embargo, una vez finalizada la misma, pueden ser de aplicación fundamentos jurídicos alternativos, tales como la existencia de plazos legales de almacenamiento.

El tratamiento de los datos se efectúa en el hardware propio ubicado en centros de datos arrendados (housing). Estos datos no se cederán a terceros. Aparte del contratista y de los representantes del cliente mencionados, ningún tercero tendrá acceso a los datos.

El fundamento jurídico para el tratamiento de esta información y de todos los datos almacenados en los servicios de Hornetsecurity es la necesidad de cumplir con la relación contractual existente.

IV. Destinatarios de datos

El tratamiento de sus datos personales en el marco de los servicios Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail se lleva a cabo en parte también por encargados de tratamiento. Estos se incluyen exclusivamente sobre la base de un contrato de tratamiento de datos en conformidad con el art. 28, apartado 3 del RGPD.

V. Transferencia de datos a terceros países

Los datos personales suyos que recogemos en el marco de Spam and Malware Protection, Hosted Exchange de Hornetsecurity, Web Filter, Hornetdrive y Control Panel y Webmail no serán transferidos a terceros países fuera del Espacio Económico Europeo.

Para el envío de SMS en el proceso de autenticación en dos pasos empleamos los servicios del proveedor Twilio, con sede en los EE.UU. y, por tanto, en un tercer país conforme al art. 44 del RPGD. Twilio trabaja conforme a cláusulas contractuales tipo de la UE certificadas, lo cual garantiza un nivel de protección de datos adecuado..

Para la administración de sus datos contractuales utilizamos los servicios del proveedor Salesforce. Salesforce trabaja de acuerdo con cláusulas contractuales tipo de la UE certificadas que garantizan un nivel adecuado de protección de datos.

Para la administración de su firma electrónica en contratos empleamos los servicios del proveedor Docusign, con sede en los EE.UU. y, por tanto, en un tercer país conforme al art. 44 del RPGD. Docusign trabaja conforme a cláusulas contractuales tipo de la UE certificadas, lo cual garantiza un nivel de protección de datos adecuado.