Datenschutzhinweise

Managed Security Services

Hornetsecurity Group

Datenschutzhinweise

für die Dienste

- 365 Total Protection (Seite 5)
- Spam and Malware Protection (Seite 6), dieser schließt die folgenden Produkte oder Dienste ein:
  - Hornetsecurity Advanced Threat Protection,
  - Hornetsecurity Email Encryption,
  - Hornetsecurity Archiving,
  - Hornetsecurity Continuity Service,
  - Hornetsecurity Signature and Disclaimer,
  - E-Mail made in Germany,
- Hornetsecurity Hosted Exchange (Seite 9)
- Web Filter (Seite 10)
- Hornetsecurity Altaro VM Backup (Seite 10)
- Hornetsecurity Altaro 365 Total Backup (Seite 11)
- Hornetdrive (Seite 11)
- Control Panel und Webmail (Seite 12)
- Test-Onboarding (Seite 12)

(nachfolgend "*Dienste*", "unsere *Dienste*" oder "die *Dienste*")

Grundlage eines effektiven Datenschutzes ist die umfassende Information über die Erhebung, Verarbeitung und Nutzung Ihrer Daten ("Datenverarbeitung"). Daher möchten wir Sie informieren,

- wann bzw. bei welchen Aktionen wir Daten verarbeiten,
- welche Daten wir aus welchen Gründen verarbeiten,
- wer Daten erhält,
- welche Rechte Sie wegen der Datenverarbeitung durch uns haben.

Diese Datenschutzhinweise beziehen sich nur auf die Nutzung personenbezogener Daten im Rahmen der *Dienste*. Diese Datenschutzhinweise können Sie dauerhaft und jederzeit herunterladen über die Adresse
https://www.hornetsecurity.com/service-privacy-statement/

I. Kontaktinformationen

Verantwortlicher für die Datenverarbeitung im Rahmen der *Dienste* im Sinne der Datenschutz-Grundverordnung (DSGVO) ist stets der Kunde. Hornetsecurity wird als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig. Die Leistungserbringung erfolgt teilweise auch durch andere Hornetsecurity-Konzernunternehmen als Unterauftragnehmer:

	Auftragsverarbeiter	Die Leistungserbringung erfolgt im inneren Unterauftragsverhältnis durch
☒	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

Wir haben zudem einen Datenschutzbeauftragten bestellt. Diesen erreichen Sie unter: datenschutz@hornetsecurity.com.

II. Allgemeines zur Datenverarbeitung

1. Umfang der Verarbeitung personenbezogener Daten

Die Bereitstellung der Dienste macht die Verarbeitung verschiedener Daten erforderlich. Darüber hinaus richtet sich der Umfang der Datenverarbeitung nach Ihrer Nutzung der Funktionalitäten der Dienste, beispielsweise welche Daten Sie dort verarbeiten bzw. verarbeiten lassen oder in die Datenverarbeitung einwilligen.

Im Rahmen des mit Hornetsecurity geschlossenen Vertrags über die Nutzung der Dienste sind Sie verpflichtet, diejenigen personenbezogenen Daten bereitzustellen, die für die Vertragserfüllung erforderlich sind. Die Weigerung, diese Daten bereitzustellen, kann eine Pflichtverletzung darstellen, aus der Sie zum Schadensersatz verpflichtet sein können. Sie sind nicht verpflichtet, uns personenbezogene Daten bereitzustellen. Soweit die Bereitstellung dieser Daten aber technisch zwingend mit der Nutzung unserer Dienste verbunden ist, führt eine Weigerung dazu, dass Sie unsere Dienste nicht nutzen können.

Bei der Nutzung der Dienste unterliegen Sie keiner automatisierten Entscheidungsfindung im Sinne von Art. 22 DSGVO.

2. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten werden nachfolgend dargestellt.

Verarbeitungsgrund	Rechtsgrundlage in der DSGVO	Erläuterung
Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen	Art. 6 Abs. 1 b)	Eine Verarbeitung erfolgt nur in dem Umfang, der für die Wahrnehmung und Erfüllung der Rechte und Pflichten aus dem Vertrag erforderlich ist. Soweit nicht ausdrücklich anders dargestellt, erfolgt die Datenverarbeitung durch uns nur in diesem Umfang.
Berechtigtes Interesse	Art. 6 Abs. 1 f)	Eine Verarbeitung erfolgt, soweit wir ein berechtigtes Interesse haben und keine entgegenstehenden überwiegenden Interessen des Betroffenen ersichtlich sind. Das konkrete Interesse wird in dieser Datenschutzhinweise im Rahmen der Verarbeitungsdarstellung erläutert.
Rechtliche Pflicht	Art. 6 Abs. 1 c)	Eine Verarbeitung erfolgt, soweit dies zur Erfüllung deutscher oder europäischer gesetzlicher Pflichten erforderlich ist.

III. Datenverarbeitung für den Betrieb der *Dienste*

Damit wir Ihnen die *Dienste* bereitstellen können, ist es erforderlich, bestimmte Daten zu verarbeiten.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

1. Grundlegende Daten

Verantwortlicher für die Verarbeitung der Stamm- und Konfigurationsdaten ist die Entität aus der Hornetsecurity Gruppe, die unter I, "Kontaktdaten", als Auftragsverarbeiter gekennzeichnet ist.

1.1. Stammdaten

Die Stammdaten des Auftraggebers (Name, Anschrift, Ansprechpartner, Telefonnummer, E-Mail-Adresse, Abteilung, Position, gebuchte Dienste, Abrechnungszeitraum, Kontoverbindung) werden zur Verwaltung der Dienste erfasst und zur Erfüllung der vertraglich vereinbarten Leistungen verwendet. Persönliche Daten von Mitbenutzern (E-Mail-Adresse) werden erfasst und zur Erfüllung der vertraglich vereinbarten Leistungen verwendet.

Die Datenverarbeitung von Mitbenutzerdaten erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Datenverarbeitung der Stammdaten des Auftraggebers werden zum Zweck der Kundenstammpflege an Unterauftragnehmer auf Systemen in einem Drittland verarbeitet (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). Die Übermittlung der Daten erfolgt auf Grundlage von Standardvertragsklauseln.

Des Weiteren werden Teile der Stammdaten des Auftraggebers zum Zwecke der Rechnungszustellung und des -versands (per Brief oder E-Mail) an Unterauftragnehmer innerhalb der EU übermittelt und auf deren Systemen verarbeitet (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Germany).

1.2. Konfigurationsdaten

Die technische Konfiguration des jeweils gebuchten *Dienstes* wird in Verbindung mit der E-Mail-Adresse des Nutzers, der Gruppenzugehörigkeit eines Benutzers oder dem Domainnamen des Kunden gespeichert.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Für Hornetsecurity Altaro VM Backup und Hornetsecurity Altaro 365 Total Backup gilt außerdem:

Für die Validierung der Lizenz werden die zur eindeutigen Identifikation erforderlichen Stammdaten (E-Mailadresse) an die Systeme der Altaro Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malta, EU, übertragen.

2. 365 Total Protection

Bei Spam and Malware Protection werden eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf den IT-Systemen des Auftragnehmers gefiltert. Es werden auch ausgehende E-Mails gefiltert.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs und der -zustellung, IP-Adressen der an der Kommunikation beteiligten Server, SMTP-Errorcode und -text), Inhalt von E-Mails und die Klassifikation der Mail (Clean, Spam, Virus, Infomail). Die Nachrichten-Metadaten werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Für die Nutzung von Individual User Signatures, Company Disclaimer und 1-Click Intelligent Ads wird der Einsatz eines Verzeichnisdienstes auf Seiten des Auftraggebers vorausgesetzt, der vom Auftragnehmer über das LDAP-Protokoll abgefragt werden kann. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein. Die Nachrichten müssen über die Relays des Auftragnehmers versendet werden.

Die automatische Datenverarbeitung umfasst die Mailadresse des Nutzers, zugeordneter Gruppenname im Verzeichnisdienst, weitere ggf. im Verzeichnisdienst verknüpfte Informationen wie Organisationszugehörigkeit, Position, Telefonnummer, Faxnummer und Mailfooter-Inhalte, die auf Seiten des Auftraggebers der Gruppe im Verzeichnis zugeordnet sind. Die personenbezogenen Daten, die dem Verzeichnis entnommen werden, werden nach Beendigung der Dienstnutzung gelöscht. Die verarbeitete Nachricht wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Global S/MIME & PGP Encryption: Der Auftragnehmer verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien. Je nach Einstellung der Richtlinien werden ausgehende E-Mails im geschützten Websafe für den Empfänger bereitgestellt.

Die automatische Datenverarbeitung umfasst die E-Mail-Adresse des Absenders und Empfängers, privater und öffentlicher S/MIME bzw. PGP-Schlüssel, ausgehende E-Mailinhalte an Dritte (Websafe), Mailadresse in Public Keys von Dritten, Status der Verschlüsselung und Inhalte von E-Mails. Die Daten Absender, Empfänger und Verschlüsselungsstatus werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

E-Mail Archiv: Der Auftragnehmer archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen.

Die automatische Datenverarbeitung umfasst die Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs, IP-Adressen der an der Kommunikation beteiligten Server, den Inhalt von E-Mails und ggf. Name und Typ des Anhangs.

Die Daten Absender- und Empfängeradresse, Mailbetreff, Datum/Uhrzeit, Anhangsname und -typ werden zur Anzeige im Control Panel verwendet. Alle diese Daten inkl. der Nachricht selber werden nach kundenspezifischer Archivdauer zzgl. 1 Jahr gespeichert und danach gelöscht. Eine Löschhemmung auf Kundenwunsch kann die Speicherdauer erhöhen.

Advanced Thread Protection (ATP): schützt den E-Mail-Verkehr des Auftraggebers vor gezielten und individuellen Angriffen, wie Spear-Phishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud. Zur Erkennung von Angriffen werden durch den Auftragnehmer als verdächtig eingestufte E-Mails des Auftraggebers durch erweiterte Filtertechniken untersucht.

Hierzu werden Metainformationen zum Mailinhalt sowie der Mailanhangstyp, -name und -inhalt automatisch verarbeitet. Die Metainformationen zum Mailinhalt werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail wird nach erfolgreicher Analyse aus dem ATP-System gelöscht.

Contingency Covering: Der Auftragnehmer stellt im Falle des Ausfalls des Zielservers je Benutzer ein E-Mail Postfach mit 10 GB Speicherplatz zur Verfügung. Auf E-Mails in diesem Postfach können autorisierte Benutzer über ein Webmail-Interface oder per IMAP und POP3 zugreifen.

Die automatische Datenverarbeitung umfasst Metadaten der Nachricht (die Mailadresse des Absenders und Empfängers, Datum/Uhrzeit des Maileingangs), Mailinhalte sowie Webmail-Metadaten (Anmeldename, IP-Adresse, Verbindungsdauer, Abrufvolumen, Protokoll). Nachrichten-Metadaten, Webmail-Metadaten und archivierte Nachrichten werden nach spätestens 14 Monaten gelöscht. Nachrichten im Webmail-Postfach werden spätestens gelöscht, wenn der Kunde den Dienst nicht mehr nutzt.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Co-location) platziert ist.

Für die Nutzung von Single-Sign-On wird bei der Anmeldung des Nutzers die E-Mail-Adresse an Microsoft weitergegeben.

Eine Weitergabe anderer Daten an Dritte erfolgt nicht, Zugriff auf die Daten durch Dritte erfolgt ebenfalls nicht.

3. Spam and Malware Protection

Bei Spam and Malware Protection werden eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf den IT-Systemen des Auftragnehmers gefiltert. Soweit der Auftraggeber es wünscht, werden auch ausgehende E-Mails gefiltert.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs

und der -zustellung, IP-Adressen der an der Kommunikation beteiligten Server, SMTP-Error-code und -text), Inhalt von E-Mails und die Klassifikation der Mail (Clean, Spam, Virus, Infomail). Die Nachrichten-Metadaten werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Co-location) platziert ist.

Eine Weitergabe anderer Daten (Mailheader, Absender, Adressat, Betreff, Datum, Textinhalt) an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.1. Optional: Advanced Thread Protection (ATP)

ATP schützt den E-Mail-Verkehr des Auftraggebers vor gezielten und individuellen Angriffen, wie Spear-Phishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud. Zur Erkennung von Angriffen werden durch den Auftragnehmer als verdächtig eingestufte E-Mails des Auftraggebers durch erweiterte Filtertechniken untersucht.

Hierzu werden Metainformationen zum Mailinhalt sowie der Mailanhangstyp, -name und -inhalt automatisch verarbeitet. Die Metainformationen zum Mailinhalt werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail wird nach erfolgreicher Analyse aus dem ATP-System gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Co-location) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.2. Optional: Email Encryption

Der Auftragnehmer bestellt und verwaltet S/MIME-Zertifikate, verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien. Je nach Einstellung der Richtlinien werden ausgehende E-Mails im geschützten Websafe für den Empfänger bereitgestellt.

Die automatische Datenverarbeitung umfasst die E-Mail-Adresse des Absenders und Empfängers, den privaten und öffentlichen S/MIME bzw. PGP-Schlüssel, Inhalte von ausgehenden Emails an Dritte (Websafe), die Mailadresse in Public Keys von Dritten, den Status der Verschlüsselung und den Inhalt der Email. Die Daten Absender, Empfänger und Verschlüsselungsstatus werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Co-location) platziert ist.

Zur Bestellung von S/MIME-Zertifikaten werden E-Mail-Adresse und Vor- und Nachname des Zertifikatsbestellers zur Verarbeitung an ein Subunternehmen in der EU übermittelt (PSW Group GmbH, Flemingstr. 20-22, 36041 Fulda, Germany).

Für eine Zwei-Faktor-Authentifizierung (2FA) des Websafe-Empfängers wird optional dessen Handy-Nummer zur Verarbeitung an einen Subunternehmer übermittelt (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, California 94105, USA). Die Übermittlung erfolgt auf Basis von Standardvertragsklauseln.

Eine Weitergabe anderer als der zur S/MIME-Zertifikatsbestellung und Generierung eines 2FA-Schlüssels genannten Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.3. Optional: Archiving

Der Auftragnehmer archiviert E-Mails des Auftraggebers revisionssicher auf seinen eigenen IT-Systemen.

Die automatische Datenverarbeitung umfasst die Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit des Maileingangs, IP-Adressen der an der Kommunikation beteiligten Server, den Inhalt von E-Mails und ggf. Name und Typ des Anhangs.

Die Daten Absender- und Empfängeradresse, Mailbetreff, Datum/Uhrzeit, Anhangsname und -typ werden zur Anzeige im Control Panel verwendet. Alle diese Daten inkl. der Nachricht selber werden nach kundenspezifischer Archivdauer zzgl. 1 Jahr gespeichert und danach gelöscht. Eine Löschhemmung auf Kundenwunsch kann die Speicherdauer erhöhen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.4. Optional: Continuity Service

Der Auftragnehmer stellt eingehende und ausgehende E-Mails des Auftraggebers für einen Zeitraum von 3 Monaten im Archiv bereit unter der Voraussetzung, dass diese E-Mails über die Server von Hornetsecurity geleitet werden.

Der Auftragnehmer stellt ferner je Benutzer ein E-Mail Postfach mit 10 GB Speicherplatz zur Verfügung. Auf E-Mails in diesem Postfach können autorisierte Benutzer über ein Webmail-Interface oder per IMAP und POP3 zugreifen.

Die automatische Datenverarbeitung umfasst Metadaten der Nachricht (die Mailadresse des Absenders und Empfängers, Datum/Uhrzeit des Maileingangs), Mailinhalte sowie Webmail-Metadaten (Anmeldename, IP-Adresse, Verbindungsdauer, Abrufvolumen, Protokoll). Nachrichten-Metadaten, Webmail-Metadaten und archivierte Nachrichten werden nach spätestens 14 Monaten gelöscht. Nachrichten im Webmail-Postfach werden spätestens gelöscht, wenn der Kunde den Dienst nicht mehr nutzt.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.5. Optional: E-Mail-Signature and Disclaimer

Für die Nutzung von Signature and Disclaimer wird der Einsatz eines Verzeichnisdienstes auf Seiten des Auftraggebers vorausgesetzt, der vom Auftragnehmer über das LDAP-Protokoll abgefragt werden kann. Zusätzlich müssen die Gruppen aus dem Benutzerverzeichnis im Control Panel organisiert sein. Die Nachrichten müssen über die Relays des Auftragnehmers versendet werden.

Die automatische Datenverarbeitung umfasst die Mailadresse des Nutzers, zugeordneter Gruppenname im Verzeichnisdienst und weitere ggf. im Verzeichnisdienst verknüpfte Informationen wie Organisationszugehörigkeit, Position, Telefonnummer, Faxnummer und Mailfooter-Inhalte, die auf Seiten des Auftraggebers der Gruppe im Verzeichnis zugeordnet sind. Die personenbezogenen Daten, die dem Verzeichnis entnommen werden, werden nach Beendigung der Dienstnutzung gelöscht. Die verarbeitete Nachricht wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

3.6. Optional: E-Mail made in Germany

Der Auftragnehmer ermöglicht eine Anbindung der E-Mail-Infrastruktur des Auftraggebers an den E-Mail made in Germany (EmiG) – Verbund und realisiert hierfür die Mailserver-seitige Umsetzung, die für die Erfüllung der Anforderungen an eine durchgehende Transportverschlüsselung von E-Mails im EmiG-Verbund notwendig ist.

Die automatische Datenverarbeitung umfasst die Metadaten der Nachrichtenübermittlung (Mailadresse des Absenders und Empfängers, Mailbetreff, Datum/Uhrzeit Maileingang, IP-Adressen der an der Kommunikation beteiligten Server, Verschlüsselungsstatus) und Inhalt von E-Mails. Die Metadaten der Nachrichtenübermittlung werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht. Die Mail selber wird nach erfolgreicher Zustellung oder Bounce gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

4. Hosted Exchange

Der Auftraggeber kann zusätzlich zum Spam and Malware Protection Hosted Exchange Postfächer buchen, wenn kein eigener Mailserver genutzt werden soll. Hosted Exchange bietet Ihnen ohne zusätzlichen Aufwand den sicheren Betrieb eines professionell verwalteten Exchange Servers in Ihrer Maildomäne mit Active Sync, gemeinsamen Kontaktinformationen, Online-Kalender, Gruppen-Collaboration und Zugriff von verschiedenen Clients und Hardware-Plattformen.

Die automatische Datenverarbeitung umfasst empfangene und gesendete E-Mails, Mailadresse des Nutzers, Gruppenmitgliedschaften, Erstellungsdatum des Postfachs, Berechtigungen von/auf andere interne Konten derselben Domäne und genutzte Mobilgeräte für Zugriff auf das Postfach. Ferner, sofern eingepflegt: Firma, Position, Abteilung, MA-Nummer, Vorgesetzter, Telefonnummern, Adresse. Die Daten werden spätestens 90 Tage nach Kündigung des Dienstes gelöscht.

E-Mails werden zur Verarbeitung und Speicherung an Server von Subunternehmen in der EU übermittelt (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Germany oder Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Germany).

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

5. Web Filter

Ausgehende http/https- und ftp-Aufrufe des Auftraggebers werden über Proxy-Server des Auftragnehmers geleitet. Datenverkehr wird auf potenziell schädliche Inhalte geprüft und ggf. ausgefiltert.

Die automatische Datenverarbeitung umfasst Datum und Uhrzeit des Aufrufs einer Webadresse, aufrufende IP-Adresse, aufgerufene URL, klassifizierte Kategorie des aufgerufenen Objekts, authentifizierte Entität: entweder E-Mail-Adresse, u.U. pseudonymisiert, oder IP-Adresse oder Verzeichnisdienst-Name und -Objektpfad oder Web Filter-Connector-String (sAMAccountName, Domain-ID, Rechnername, Rechner-IP, aufrufendes Programm). Die genannten Daten (URL ohne Pfad) werden zur Anzeige im Control Panel verwendet und nach spätestens 14 Monaten gelöscht.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

6. Hornetsecurity Altaro VM Backup

Hornetsecurity Altaro VM Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Backup- und Wiederherstellungslösung für virtualisierte Server in Hyper-V und VMware-Umgebungen sowie physische Microsoft Server.

Hornetsecurity Altaro VM Backup ermöglicht dem Kunden die Durchführung von Backups auf die vom Kunden festgelegten Orte in den vom Kunden festgelegten Zeitintervallen. Die Verschlüsselung der Backups wird durch vom Kunden konfigurierte AES-256-Verschlüsselungsschlüssel (Passwort) sichergestellt. Alle Offsite-Kopien sind AES-256-verschlüsselt. Für Onsite-Backups (primär) ist die Verschlüsselung optional und wird ebenfalls unterstützt.

Für Offsite-Kopien erfolgt optional eine Datenspeicherung auf durch den Kunden bei Drittanbietern angemietetem Cloud-Speicher (Microsoft Azure Blob Storage oder Wasabi Cloud Object Storage oder Amazon S3). Der Kunde agiert als Auftraggeber gegenüber den Drittanbietern.

Während des Betriebs wird die eingesetzte Softwarelizenz online mit der in den Stammdaten hinterlegten erworbenen Lizenz abgeglichen. Eine Übertragung an oder Verarbeitung der Nutzdaten der Dienste durch den Auftragnehmer erfolgt nicht.

7. Hornetsecurity Altaro 365 Total Backup

Hornetsecurity Altaro 365 Total Backup ist eine zuverlässige, intuitive und einfach zu verwaltende Sicherungs- und Wiederherstellungslösung für Microsoft 365 Mailboxen, OneDrive—Konten für Unternehmen, SharePoint-Dokumentbibliotheken, Teams-Chats und Endpoints.

Hornetsecurity Altaro 365 Total Backup ermöglicht dem Kunden über eine Multi-Tenant-Konsole eine richtlinienbasierte Konfiguration, Übersicht und Überwachung von Rechten, Sicherungen und zu sichernden MS365 Objekten Alle Backup-Daten sind mit kundenindividuellen AES-256-Schlüsseln verschlüsselt.

Die Datenverwaltung der gesicherten und verschlüsselten Daten erfolgt in der Hornetsecurity Gruppe konzernintern durch Altaro Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malta ("Altaro"). Die Speicherung der verschlüsselten Backup-Daten erfolgt durch Altaro in der Microsoft Azure Cloud, Zone Westeuropa, wo Altaro die Microsoft Azure-Plattform und Compliance-Services nutzt. Die Azure Westeuropa Cloud Plattform und Services sind zertifiziert nach SOC 1 Type 2, SOC 2 Type 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS and HIPAA.

Während des Betriebs wird die eingesetzte Softwarelizenz online mit der in den Stammdaten hinterlegten erworbenen Lizenz abgeglichen. Eine Übertragung an oder Verarbeitung der Nutzdaten der Dienste durch den Auftragnehmer erfolgt nicht.

8. Hornetdrive

Hornetdrive ermöglicht die verschlüsselte Speicherung, Austausch und gemeinsame Bearbeitung von Dateien in der Cloud.

Die automatische Datenverarbeitung umfasst die angemeldete E-Mail-Adresse, Datum der Ersteinrichtung, Name der verwendeten Geräte, Datum des erstmaligen und letzten Zugriffs von diesem Gerät, Betriebssystemversion des Geräts, Drivenamen der angelegten Drives und Erstellungsdatum, genutztes Drivevolumen, Summe belegter Speicherplatz und verschlüsselte Dateiinhalte des Nutzers.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

9. Anmeldung am Control Panel und Webmail

Wenn Sie bereits Kunde von Hornetsecurity sind, können Sie sich über unsere Website im Control Panel, von dem aus Sie Ihre Leistung nutzen und verwalten können, anmelden. Als Kunde von Webmail können Sie sich über einen separaten Link in Ihrem Postfach anmelden. Für die Anmeldung benötigen Sie jeweils Ihren Benutzernamen bzw. Ihre E-Mail-Adresse sowie Ihr Password. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

Die Datenverarbeitung erfolgt auf eigener Hardware, die in angemieteten Rechenzentren (Colocation) platziert ist. Eine Weitergabe der Daten an Dritte erfolgt nicht. Neben dem Auftragnehmer und benannten Vertretern des Auftraggebers haben keine Dritten auf die Daten Zugriff.

Die Rechtsgrundlage der Verarbeitung dieser Informationen und gespeicherten Daten ist die Erforderlichkeit zur Erfüllung der bestehenden Vertragsbeziehung.

10. Test-Onboarding

Um die Leistung der Dienste zu testen, können Sie sich direkt über unsere Website anmelden. Hierfür benötigen wir verschiedene Informationen zu Ihnen persönlich, zu Domäne, Server und Nutzer, für welche die Leistung gewünscht ist, sowie zum gewünschten Service. Die Pflichtfelder sind entsprechend gekennzeichnet. Alle weiteren Informationen erfolgen freiwillig. Die Speicherdauer bemisst sich entsprechend grundsätzlich an der Dauer der Vertragsbeziehung. Nach deren Ende können aber alternative Rechtsgrundlagen eingreifen, wie etwa gesetzliche Speicherfristen.

Die Datenverarbeitung der Stammdaten des Auftraggebers werden zum Zweck der Kundenstammpflege an Unterauftragnehmer auf Systemen in einem Drittland verarbeitet (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, USA). Die Übermittlung der Daten erfolgt auf Grundlage von Standardvertragsklauseln.

Rechtsgrundlage der Verarbeitung ist insoweit die Durchführung vorvertraglicher Maßnahmen bzw. die Erforderlichkeit für die Vertragserfüllung.

IV. Widerspruchs- und Beseitigungsmöglichkeit

Soweit die Datenverarbeitung auf Ihrer Einwilligung oder unserem berechtigten Interesse basiert, haben Sie jederzeit das Recht, der Verarbeitung zu widersprechen oder Ihre erteilte Einwilligung zu widerrufen. Ihr Widerspruch bzw. Widerruf hat lediglich Wirkung für die Zukunft. Sie können sich jederzeit zur Ausübung Ihres Widerspruchs- oder Widerrufsrechts an datenschutz@hornetsecurity.com wenden. Wenn Sie einer Verarbeitung aufgrund unseres berechtigten Interesses widersprechen, dürfen wir die Verarbeitung dennoch fortführen, wenn wir zwingende schutzwürdige Gründe für die Verarbeitung nachweisen können, die Ihre Interessen, Rechte und Freiheiten überwiegen.

V. Betroffenenrechte

Werden auf Ihre Person bezogenen Daten verarbeitet, sind Sie Betroffener im Sinne von Art. 4 Abs. 1 DSGVO. Als Betroffenem stehen Ihnen in Bezug auf Ihre personenbezogenen Daten die nachfolgenden Rechte zu. Zur Ausübung dieser Rechte können Sie sich unter den oben angegebenen Kontaktdaten an uns wenden.

Recht auf Auskunft nach Art. 15 DSGVO

Sie haben ein Recht auf Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten. Dies umfasst die in Art. 15 DSGVO dargestellten Pflichtinformationen.

Recht auf Berichtigung nach Art. 16 DSGVO

Sie haben das Recht, die unverzügliche Berichtigung falscher sowie die Vervollständigung unrichtiger personenbezogener Daten.

Recht auf Löschung nach Art. 17 DSGVO

Sie haben das Recht, die Löschung Ihrer personenbezogenen Daten zu verlangen, wenn einer der in Art. 17 DSGVO genannten Gründe eingreift, insbesondere, wenn keine Rechtsgrundlage mehr für die Verarbeitung vorliegt.

Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO

Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn einer der in Art. 18 DSGVO genannten Gründe eingreift, insbesondere auf Ihren Wunsch hin statt einer Löschung der Daten.

Recht auf Datenübertragbarkeit nach Art. 20 DSGVO

Sie haben das Recht, alle bei uns über Sie gespeicherten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format herauszuverlangen und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, Art. 77 DSGVO

Sie haben gemäß Art. 77 DSGVO das Recht, eine Beschwerde bei der für Sie zuständigen Aufsichtsbehörde einzureichen.

VI. Empfänger von Daten

Die Verarbeitung Ihrer personenbezogenen Daten im Rahmen der *Dienste* erfolgt zum Teil auch durch Auftragsverarbeiter. Diese werden ausschließlich auf der Grundlage einer Vereinbarung zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO einbezogen.

VII. Datenübermittlung in Drittländer

Die personenbezogenen Daten, die wir von Ihnen im Rahmen der Leistungserbringung der *Dienste* erheben, werden nicht in Drittländer außerhalb des Europäischen Wirtschaftsraumes übermittelt.

Für den SMS-Versand einer Zwei-Faktor-Authentifizierung nutzen wir den Anbieter Twilio. mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Twilio ist nach Standardvertragsklauseln zertifizierten, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.

Für die Verwaltung Ihrer Vertragsdaten nutzen wir den Anbieter Salesforce mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Salesforce arbeitet nach zertifizierten Standardvertragsklauseln, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.

Für die Verwaltung Ihrer elektronischen Unterschrift bei Verträgen nutzen wir den Anbieter Docusign mit Sitz in den USA und damit in einem Drittland gemäß Art. 44 DSGVO. Docusign arbeitet nach zertifizierten Standardvertragsklauseln, wodurch ein angemessenes Datenschutzniveau gewährleistet wird.