Remarques sur la protection des données

Services de sécurité gérés

Hornetsecurity Group

Remarques sur la protection des données

pour les services suivants :

- 365 Total Protection (page 5)
- Spam and Malware Protection (page 7), incluant les produits ou services suivants :
  - Hornetsecurity Advanced Threat Protection (page 7)
  - Hornetsecurity Email Encryption (page 7)
  - Hornetsecurity Email Archiving (page 8)
  - Hornetsecurity Continuity Service (page 8)
  - Hornetsecurity Signature and Disclaimer (page 9)
  - E-Mail made in Germany (page 9)
- Hornetsecurity Hosted Exchange (page 10)
- Web Filter (page 10)
- Hornetsecurity Altaro VM Backup (page 11)
- Hornetsecurity Altaro 365 Total Backup (page 11)
- Hornetdrive (page 11)
- Control Panel et Webmail (page 12)
- Intégration pour l'essai (page 12)

(ci-après, les « services » ou le « service »)

La base d'une protection efficace des données est une information complète sur la collecte, du traitement et de l'utilisation de vos données (« traitement des données »). Par conséquent, nous souhaitons vous informer sur les points suivants :

- quand ou pendant quelles actions nous traitons les données;
- quelles données nous traitons et pour quelles raisons;
- qui reçoit les données;
- de quels droits vous disposez suite au traitement des données effectué par nos soins.

Les présentes remarques sur la protection des données se fondent uniquement sur l'utilisation de données à caractère personnel dans le cadre des services. Vous pouvez télécharger ces informations sur la protection des données à tout moment à l'adresse suivante :
https://www.hornetsecurity.com/service-privacy-statement/

I. Coordonnées

Au sens du Règlement général sur la protection des données (RGPD), le client est toujours la personne responsable du traitement des données dans le cadre des services. Hornetsecurity agit en tant que sous-traitant au sens de l'article 28 du RGPD. Certains des services sont également fournis par d'autres sociétés de Hornetsecurity Group en tant que sous-traitants :

	Sous-traitant	Les services sont fournis dans le cadre d'un rapport de sous-traitance interne par
☒	Hornetsecurity GmbH Am Listholze 78 30177, Hanovre Allemagne Téléphone : +49 511 515 464-0 Courriel : info@hornetsecurity.com	-/-
☐	Hornetsecurity Iberia S.L Calle Arte 15, 1ª 28033, Madrid Espagne Tél. : +34 91 368 77 33 Courriel : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177, Hanovre Allemagne Tél. : +49 511 515 464-0 Courriel : info@hornetsecurity.com
☐	Aegis Security Argentina S.A. Belgrano 53 Piso, PB Dpto : B Tandil, Buenos Aires Argentine Tél. : +54 9 249 449 9296 Courriel : info@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177, Hanovre Allemagne Tél. : +49 511 515 464-0 Courriel : info@hornetsecurity.com
☐	Hornetsecurity Ltd. 55 Baker Street Londres, W1U7EU Royaume-Uni Tél. : +44 203 0869 833 Courriel : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177, Hanovre Allemagne Tél. : +49 511 515 464-0 Courriel : info@hornetsecurity.com
☐	Hornetsecurity Inc. 6425 Living Place, Suite 200 Pittsburgh, PA 15206 États-Unis Tél. : +1 (412) 924-5300 Courriel : sales@hornetsecurity.com	Hornetsecurity GmbH Am Listholze 78 30177, Hanovre Allemagne Tél. : +49 511 515 464-0 Courriel : info@hornetsecurity.com

De plus, nous avons nommé un délégué à la protection des données. Vous pouvez le contacter à l'adresse privacy@hornetsecurity.com.

II. Généralités sur le traitement des données

1. Étendue du traitement des données à caractère personnel

La fourniture des services nécessite le traitement de diverses données. En outre, l'étendue du traitement des données dépend de votre utilisation des fonctionnalités des services, par ex., des données que vous y traitez ou faites traiter ou de votre consentement au traitement des données.

Dans le cadre du contrat conclu avec Hornetsecurity pour l'utilisation des services, vous êtes tenu(e) de fournir les données à caractère personnel qui sont nécessaires à l'exécution du contrat. Le refus de fournir ces données peut constituer une violation d'obligation pouvant vous contraindre à une indemnisation. Vous n'êtes pas obligé(e) de nous fournir des données à caractère personnel. Toutefois, si la fourniture de ces données est techniquement obligatoire pour l'utilisation de nos services, un refus aura pour conséquence de vous empêcher d'utiliser nos services.

Lors de l'utilisation des services, vous n'êtes pas soumis(e) à une prise de décision automatisée au sens de l'article 22 du RGPD.

2. Base juridique du traitement des données à caractère personnel

Les bases juridiques du traitement des données à caractère personnel sont présentées ci-dessous.

Raison du traitement	Base juridique dans le RGPD	Explication
Exécution du contrat ou de mesures précontractuelles	Art. 6 alinéa 1 b)	Le traitement n'est effectué que dans la mesure nécessaire à l'exercice et à l'exécution des droits et obligations résultant du contrat. Sauf mention contraire expresse, nous ne traitons les données que dans cette mesure.
Intérêt légitime	Art. 6 alinéa 1 f)	Le traitement a lieu dans la mesure où nous y avons un intérêt légitime et où aucun intérêt prépondérant contraire de la personne concernée n'est apparent. L'intérêt concret est expliqué dans les présentes remarques sur la protection des données dans le cadre de la description du traitement.
Obligation légale	Art. 6 alinéa 1 c)	Le traitement a lieu dans la mesure où il est nécessaire à la satisfaction d'obligations légales allemandes ou européennes.

III. Traitement des données pour le fonctionnement des services

Pour que nous puissions mettre à votre disposition les services, il est nécessaire de traiter certaines données.
La base légale pour le traitement de ces informations et données stockées est la nécessité de satisfaire la relation contractuelle existante. Par conséquent, la durée de conservation est généralement mesurée en fonction de la durée de la relation contractuelle. Toutefois, lorsque celle-ci prend fin, d'autres bases juridiques peuvent intervenir, telles que les délais de conservation légaux.

1. Données fondamentales

L'entité responsable du traitement des données de base et de configuration est l'entité du Hornetsecurity Group, qui est identifiée comme le sous-traitant au point I, « Coordonnées ».

1.1. Données maîtres

Les données maîtres du client (nom, adresse, interlocuteur, numéro de téléphone, adresse électronique, département, poste, services commandés, période de facturation, coordonnées bancaires) sont enregistrées pour l'administration des services et utilisées pour exécuter les services convenus contractuellement. Les données personnelles des co-utilisateurs (adresse courriel) sont collectées et utilisées pour l'exécution des services convenus contractuellement.

Le traitement des données des utilisateurs partagés est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

Les données maîtres du client sont traitées à des fins de gestion des données par des sous-traitants sur des systèmes dans un pays tiers (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, États-Unis). La transmission des données se fonde sur des clauses contractuelles types.

En outre, certaines parties des données de la base de clients sont transmises à un sous-traitant au sein de l'UE (PIN Mail AG, Alt-Moabit 91, 10559 Berlin, Allemagne) à des fins de livraison et d'expédition des factures (par courrier ou par courriel) et traitées sur leurs systèmes.

1.2. Données de configuration

La configuration technique du service commandé est enregistrée en relation avec l'adresse courriel de l'utilisateur, l'appartenance à un groupe d'utilisateurs ou le nom de domaine du client.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

Pour Hornetsecurity Altaro VM Backup et Hornetsecurity Altaro 365 Total Backup s'appliquent également les précisions suivantes :

Pour la validation de la licence, les données maîtres (adresse courriel) nécessaires à l'identification unique sont transférées aux systèmes d'Altaro Limited, Block LS3, Level 1, Malta Life Sciences Park, San Gwann Industrial Estate, San Gwann SGN 3000, Malte, UE.

2. 365 Total Protection

Le filtre Spam and Malware Protection examine les courriels entrants du client pour détecter les contenus nuisibles (par ex., les virus), les publicités indésirables (par ex., les spams) et les publicités légitimes (par ex., les infolettres) sur les systèmes informatiques du prestataire. Les courriels sortants sont également filtrés.

Le traitement automatique des données comprend les métadonnées de la transmission du message (adresse courriel de l'expéditeur et du destinataire, objet du courriel, date et heure de réception et de distribution du courriel, adresses IP des serveurs impliqués dans la communication, code et texte de l'erreur SMTP), le contenu du courriel et sa classification (Valide, Spam, Virus, Infomail). Les métadonnées des messages sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel lui-même est effacé après une distribution réussie ou retournée.

L'utilisation de signatures individuelles propres aux utilisateurs, d'un avis de non-responsabilité de l'entreprise ou de pubs intelligentes en un clic nécessite l'utilisation d'un service d'annuaire du côté du client, qui peut être interrogé par le contractant via le protocole LDAP. En outre, les groupes du répertoire des utilisateurs doivent être organisés dans le Control Panel. Les messages doivent être envoyés via les relais du prestataire.

Le traitement automatique des données comprend l'adresse courriel de l'utilisateur, le nom de groupe attribué dans le service de répertoire et d'autres informations éventuellement liées dans le service de répertoire, telles que l'appartenance organisationnelle, le poste, le numéro de téléphone, le numéro de télécopieur et le contenu du pied de page du courriel, qui sont attribuées au groupe dans le répertoire du client. Les données à caractère personnel tirées du répertoire sont supprimées après la fin de l'utilisation du service. Le message traité est effacé après une distribution réussie ou retournée.

Chiffrement global S/MIME et PGP : Le prestataire crypte et signe les courriels sortants et décrypte les courriels entrants du client sur ses propres systèmes informatiques conformément aux directives définies. Selon les paramètres réglés, les courriels sortants sont fournis au destinataire dans un coffre-fort Web sécurisé (« Websafe »).

Le traitement automatique des données comprend l'adresse courriel de l'expéditeur et du destinataire, la clé privée et publique S/MIME ou PGP, le contenu des courriels envoyés à des tiers (Websafe), l'adresse courriel dans les clés publiques des tiers, l'état du cryptage et le contenu du courriel. Les données relatives à l'expéditeur, au destinataire et à l'état du cryptage sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel lui-même est effacé après une distribution réussie ou retournée.

L'archivage des courriels : Le prestataire archive les courriels du client de manière irréprochable sur ses propres systèmes informatiques.

Le traitement automatique des données comprend l'adresse courriel de l'expéditeur et du destinataire, l'objet du courriel, la date et l'heure de réception du courriel, les adresses IP des serveurs impliqués dans la communication et, le cas échéant, le nom et le format de la pièce jointe.

L'adresse courriel de l'expéditeur et du destinataire des données, l'objet du courriel, la date/l'heure ainsi que le nom et le format de la pièce jointe sont utilisés pour l'affichage dans le Control Panel. Toutes ces données, y compris le message lui-même, sont stockées selon la durée d'archivage propre au client, plus 1 an, puis effacées. Une inhibition de la suppression à la demande du client peut augmenter la durée de conservation.

Advanced Thread Protection (ATP) : Le service ATP protège le trafic de messagerie du client contre les attaques ciblées et individuelles (harponnage, attaques mixtes, menaces persistantes évoluées, rançongiciels et fraudes du président, notamment). Afin de détecter les attaques, les courriels du client classés comme suspects sont examinés par le prestataire à l'aide de techniques de filtrage avancées.

À cette fin, les méta-informations sur le contenu du courriel ainsi que le format, le nom et le contenu de la pièce jointe sont automatiquement traités. Ces méta-informations sur le contenu du courriel sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel est effacé du système ATP après une analyse réussie.

Continuity Service : En cas de défaillance du serveur cible, le prestataire doit également fournir une boîte de réception électronique courriel d'une capacité de stockage de 10 Go par utilisateur, dans l'éventualité d'une défaillance du serveur cible. Les utilisateurs autorisés peuvent accéder aux courriels de cette boîte de réception via une interface de messagerie Web ou via IMAP et POP3.

Le traitement automatique des données comprend les métadonnées du message (adresse courriel de l'expéditeur et du destinataire, date et heure de réception du courriel), le contenu du courriel et les métadonnées de la messagerie Web (nom de connexion, adresse IP, durée de la connexion, volume de consultation, journal). Les métadonnées des messages, les métadonnées de la messagerie Web et les messages archivés sont supprimés au plus tard après 14 mois. Les messages de la boîte de réception Web sont supprimés au plus tard lorsque le client n'utilise plus le service.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation).

Dans le cas de l'utilisation de l'authentification unique, l'adresse courriel est transmise à Microsoft lors de l'inscription de l'utilisateur.

Les données ne sont pas transmises à des tiers, l'accès aux données par des tiers n'a pas lieu non plus.

Juridiquement, ces informations et les données stockées sont traitées pour le seul motif de satisfaire la relation contractuelle existante.

3. Spam and Malware Protection

Ce service filtre les courriels entrants du client pour détecter les contenus nuisibles (par ex., les virus), les publicités indésirables (par ex., les spams) et les publicités légitimes (par ex., les infolettres) sur les systèmes informatiques du prestataire. Si le client le souhaite, les courriels sortants sont également filtrés.

Le traitement automatique des données comprend les métadonnées de la transmission du message (adresse courriel de l'expéditeur et du destinataire, objet du courriel, date et heure de réception et de distribution du courriel, adresses IP des serveurs impliqués dans la communication, code et texte de l'erreur SMTP), le contenu du courriel et sa classification (Valide, Spam, Virus, Infomail). Les métadonnées des messages sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel lui-même est effacé après une distribution réussie ou retournée.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation).

Les autres données (en-tête du courriel, expéditeur, destinataire, objet, date, contenu du texte) ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.1. En option : Advanced Thread Protection (ATP)

Le service ATP protège le trafic de messagerie du client contre les attaques ciblées et individuelles (harponnage, attaques mixtes, menaces persistantes évoluées, ransomware rançongiciels et fraudes du président, notamment). Afin de détecter les attaques, les courriels du client classés comme suspects sont examinés par le prestataire à l'aide de techniques de filtrage avancées.

À cette fin, les méta-informations sur le contenu du courriel ainsi que le format, le nom et le contenu de la pièce jointe sont automatiquement traités. Ces méta-informations sur le contenu du courriel sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel est effacé du système ATP après une analyse réussie. Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.2. En option : Email Encryption

Le prestataire commande et gère les certificats S/MIME, crypte et signe les courriels sortants et décrypte les courriels entrants du client sur ses propres systèmes informatiques conformément aux directives définies. Selon les paramètres réglés, les courriels sortants sont fournis au destinataire dans un coffre-fort Web sécurisé (« Websafe »).

Le traitement automatique des données comprend l'adresse courriel de l'expéditeur et du destinataire, la clé privée et publique S/MIME ou PGP, le contenu des courriels envoyés à des tiers (Websafe), l'adresse courriel dans les clés publiques des tiers, l'état du cryptage et le contenu du courriel. Les données relatives à l'expéditeur, au destinataire et à l'état du cryptage

sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel lui-même est effacé après une distribution réussie ou retournée.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation).

Pour commander des certificats S/MIME, l'adresse courriel et les nom et prénom du demandeur de certificat sont transmis à un sous-traitant situé dans l'UE pour y être traités (PSW Group GmbH, Flemingstr. 20-22, 36041 Fulda, Allemagne).

Pour l'authentification à deux facteurs (2FA) du destinataire Websafe, le numéro de téléphone mobile du destinataire peut être transmis à un sous-traitant à des fins de traitement (Twilio Inc., 375 Beale Street, Suite 300, San Francisco, Californie 94105, États-Unis). La transmission a lieu sur la base de clauses contractuelles types.

Aucune donnée autre que celles permettant de commander le certificat S/MIME et de générer une clé 2FA ne sera transmise à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.3. En option : Email Archiving

Le prestataire archive les courriels du client de manière irréprochable sur ses propres systèmes informatiques.

Le traitement automatique des données comprend l'adresse courriel de l'expéditeur et du destinataire, l'objet du courriel, la date et l'heure de réception du courriel, les adresses IP des serveurs impliqués dans la communication et, le cas échéant, le nom et le format de la pièce jointe.

L'adresse courriel de l'expéditeur et du destinataire des données, l'objet du courriel, la date/l'heure ainsi que le nom et le format de la pièce jointe sont utilisés pour l'affichage dans le Control Panel. Toutes ces données, y compris le message lui-même, sont stockées selon la durée d'archivage propre au client, plus 1 an, puis effacées. Une inhibition de la suppression à la demande du client peut augmenter la durée de conservation. Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.4. En option : Continuity Service

Le prestataire met à disposition les courriels entrants et sortants du client pour une période de trois mois dans les archives à condition que ces courriels soient acheminés via les serveurs de Hornetsecurity.

Le prestataire doit également fournir une boîte de réception électronique 10 Go par utilisateur. Les utilisateurs autorisés peuvent accéder aux courriels de cette boîte de réception via une interface de messagerie Web ou via IMAP et POP3.

Le traitement automatique des données comprend les métadonnées du message (adresse courriel de l'expéditeur et du destinataire, date et heure de réception du courriel), le contenu du courriel et les métadonnées de la messagerie Web (nom de connexion, adresse IP, durée

de la connexion, volume de consultation, journal). Les métadonnées des messages, les métadonnées de la messagerie Web et les messages archivés sont supprimés au plus tard après 14 mois. Les messages de la boîte de réception Web sont supprimés au plus tard lorsque le client n'utilise plus le service.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.5. En option : Signature and Disclaimer

L'utilisation d'un service d'annuaire par le client est requise pour l'emploi de Signature and Disclaimer, lequel pouvant être consulté par le prestataire via le protocole LDAP. En outre, les groupes du répertoire d'utilisateurs doivent être organisés dans le Control Panel. Les messages doivent être envoyés via les relais du prestataire.

Le traitement automatique des données comprend l'adresse courriel de l'utilisateur, le nom de groupe attribué dans le service de répertoire et d'autres informations éventuellement liées dans le service de répertoire, telles que l'appartenance organisationnelle, le poste, le numéro de téléphone, le numéro de télécopieur et le contenu du pied de page du courriel, qui sont attribuées au groupe dans le répertoire du client. Les données à caractère personnel tirées du répertoire sont supprimées après la fin de l'utilisation du service. Le message traité est effacé après une distribution réussie ou retournée.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

3.6. En option : E-Mail made in Germany

Le prestataire permet la connexion de l'infrastructure de messagerie électronique du client au réseau E-Mail made in Germany (EmiG) et réalise l'implémentation correspondante du côté du serveur de messagerie, ce qui est nécessaire pour répondre aux exigences d'un cryptage de transport continu des courriels dans le réseau EmiG.

Le traitement automatique des données comprend les métadonnées de la transmission du message (adresse courriel de l'expéditeur et du destinataire, objet du courriel, date/heure de réception du courriel, adresses IP des serveurs impliqués dans la communication, état du cryptage) et le contenu du courriel. Les métadonnées de la transmission des messages sont utilisées pour l'affichage dans le Control Panel et sont effacées au plus tard après 14 mois. Le courriel lui-même est effacé après une distribution réussie ou retournée.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

4. Hosted Exchange

Le client peut réserver des boîtes de réception Hosted Exchange hébergées en plus de la Spam and Malware Protection si aucun serveur de messagerie électronique propre ne doit être utilisé. Hosted Exchange vous offre le fonctionnement sécurisé d'un serveur Exchange géré par des professionnels dans votre domaine de messagerie avec Active Sync, des informations de contact partagées, un calendrier en ligne, une collaboration de groupe et un accès à partir de plusieurs clients et plateformes matérielles, sans frais supplémentaires.

Le traitement automatique des données comprend les courriels reçus et envoyés, l'adresse courriel de l'utilisateur, les appartenances à des groupes, la date de création de la boîte de réception, les autorisations depuis/vers d'autres comptes internes du même domaine et les appareils mobiles utilisés pour accéder à la boîte de réception. Il comprend également les données suivantes dès lors qu'elles sont connues : société, poste, département, numéro d'employé, supérieur hiérarchique, numéros de téléphone, adresse. Les données sont supprimées au plus tard 90 jours après la fin du service.

Les courriels sont transmis aux serveurs de sous-traitants situés dans l'UE pour y être traités et stockés (QualityHosting AG, Uferweg 40-42, 63571 Gelnhausen, Allemagne ou Skyfillers GmbH, Schiffbrücke 66, 24939 Flensburg, Allemagne).

La base légale pour le traitement de ces informations et données stockées est la nécessité de satisfaire la relation contractuelle existante.

5. Web Filter

Les appels sortants http/https et ftp du client sont acheminés via les serveurs proxy du prestataire. Le trafic de données est vérifié pour détecter tout contenu potentiellement dangereux et est filtré si nécessaire.

Le traitement automatique des données comprend la date et l'heure de l'appel d'une adresse Web, l'adresse IP appelante, l'URL consultée, la catégorie classée de l'objet consulté, l'entité authentifiée; soit l'adresse courriel, éventuellement pseudonymisée, soit l'adresse IP, soit le nom du service d'annuaire et le chemin de fichier de l'objet, soit le Filter Connector String (sAMAccountName, ID de domaine, nom de l'ordinateur, IP de l'ordinateur, programme consultant). Ces données mentionnées (URL sans chemin) sont utilisées pour l'affichage dans le Control Panel et sont supprimées au plus tard après 14 mois.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

La base légale pour le traitement de ces informations et données stockées est la nécessité de satisfaire la relation contractuelle existante.

6. Hornetsecurity Altaro VM Backup

Hornetsecurity Altaro VM Backup une solution de sauvegarde et de restauration des données fiable, intuitive et facile à gérer pour les serveurs virtualisés dans les environnements Hyper-V et VMware ainsi que pour les serveurs physiques Microsoft.

La solution permet au client d'effectuer des sauvegardes sur des emplacements spécifiés par le client aux intervalles également spécifiés par le client. Le cryptage des sauvegardes est assuré par des clés de cryptage AES-256 (mot de passe) configurées par le client. Toutes les copies hors site sont cryptées en AES-256. Pour les sauvegardes sur site (primaires), le cryptage est facultatif et est également pris en charge.

Pour les copies hors site, les données sont éventuellement stockées sur un support de stockage en cloud loué par le client auprès de fournisseurs tiers (Microsoft Azure Blob Storage ou Wasabi Cloud Object Storage ou Amazon S3). Le client est responsable du traitement des données vis-à-vis des fournisseurs tiers.

Pendant l'exploitation, la licence du logiciel qui est utilisée est comparée en ligne avec la licence achetée et stockée dans les données maîtres. Le prestataire ne procède ni à la transmission ni au traitement des données de l'utilisateur des services.

7. Hornetsecurity Altaro 365 Total Backup

Avec Hornetsecurity Altaro 365 Total Backup une solution de sauvegarde et de récupération fiable, intuitive et facile à gérer pour les boîtes aux lettres Microsoft 365, les comptes professionnels OneDrive, les bibliothèques de documents SharePoint ainsi que les chats et les terminaux Teams.

La solution fournit aux clients une configuration, une visibilité et une surveillance basées sur des politiques des autorisations, des sauvegardes et des objets MS365 à sauvegarder via une console multilocataire. Toutes les données de sauvegarde sont cryptées avec des clés AES-256 spécifiques au client.

Au sein de Hornetsecurity Group, la gestion des données sécurisées et cryptées est effectuée par Altaro Limited, Block LS3, Level 1, Life Science Park, San Gwann Industrial Estate, San Gwann, SGN 3000, Malte (« Altaro »). Altaro stocke les sauvegardes chiffrées dans le nuage Microsoft Azure, zone Europe de l'Ouest, et utilise la plateforme et les services de conformité Microsoft Azure. La plateforme et les services infonuagiques d'Azure en Europe de l'Ouest sont certifiés SOC 1 Type 2, SOC 2 Type 2, ISO 9001, ISO 27001, ISO 22301, PCI DSS et HIPAA.

Pendant l'exploitation, la licence du logiciel qui est utilisée est comparée en ligne avec la licence achetée et stockée dans les données maîtres. Il n'y a pas de transmission ou de traitement des données de l'utilisateur des *Services* par le prestataire.

8. Hornetdrive

Hornetdrive permet le stockage crypté, le partage et l'édition collaborative de fichiers dans le nuage.

Le traitement automatique des données comprend l'adresse courriel enregistrée, la date de la configuration initiale, le nom des appareils utilisés, la date du premier et du dernier accès à partir de cet appareil, la version du système d'exploitation du dispositif, les noms des lecteurs créés et la date de création, le volume du lecteur utilisé, l'espace de stockage total utilisé et le contenu des fichiers cryptés de l'utilisateur.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

La base légale pour le traitement de ces informations et données stockées est la nécessité de satisfaire la relation contractuelle existante.

9. Connexion au Control Panel et Webmail

Si vous êtes déjà un client de Hornetsecurity, vous pouvez vous connecter au Control Panel à partir de notre site Web. Dans celui-ci, vous pouvez utiliser et gérer le service que vous avez choisi. En tant que client de messagerie Web, vous pouvez vous connecter à votre boîte de réception grâce à un lien distinct. Pour la connexion, vous avez besoin de votre nom d'utilisateur ou de votre adresse courriel ainsi que de votre mot de passe. Par conséquent, la durée de conservation est généralement mesurée en fonction de la durée de la relation contractuelle. Toutefois, lorsque celle-ci prend fin, d'autres bases juridiques peuvent intervenir, telles que les délais de conservation légaux.

Le traitement des données est effectué sur notre propre matériel, qui est situé dans des centres de données loués (colocation). Les données ne sont pas transmises à des tiers. En dehors du prestataire et des représentants désignés du client, aucun tiers n'a accès aux données.

La base légale pour le traitement de ces informations et données stockées est la nécessité de satisfaire la relation contractuelle existante.

10. Intégration pour l'essai

Pour tester les performances des services, vous pouvez vous connecter directement à notre site Web. À cette fin, nous avons besoin de diverses informations personnelles sur vous, sur le domaine, le serveur et l'utilisateur pour lesquels le service est souhaité, ainsi que sur le service souhaité. Les champs obligatoires sont marqués en conséquence. Toutes les autres informations sont facultatives. Par conséquent, la durée de conservation est généralement mesurée en fonction de la durée de la relation contractuelle. Toutefois, lorsque celle-ci prend fin, d'autres bases juridiques peuvent intervenir, telles que les délais de conservation légaux.

Les données de base du client sont traitées afin de permettre la gestion de ces données par des sous-traitants sur des systèmes dans un pays tiers (Salesforce.com, Inc., The Landmark @ One Market Street, San Francisco, CA 94105, États-Unis). La transmission des données se fonde sur des clauses contractuelles types.

La base juridique du traitement à cet égard est la mise en œuvre de mesures précontractuelles ou la nécessité de l'exécution du contrat.

IV. Destinataires de vos données

Le traitement de vos données à caractère personnel dans le cadre des services est également effectué en partie par des tierces parties. Celles-ci ne sont incluses que sur la base d'un accord de traitement commandé conformément à l'article 28, alinéa 3 du RGPD.

V. Transmission de données vers des pays tiers

Les données à caractère personnel que nous recueillons auprès de vous dans le cadre des services ne sont pas transmises à des pays tiers en dehors de l'Espace économique européen.

Pour la gestion de vos données contractuelles, nous faisons appel au prestataire Salesforce basé aux États-Unis, et donc dans un pays tiers, conformément à l'article 44 du RGPD. Salesforce est certifié selon les clauses contractuelles types.

VI. Possibilité d'opposition et de révocation

Dans la mesure où le traitement des données est fondé sur votre consentement ou sur notre intérêt légitime, vous avez le droit de vous opposer au traitement à tout moment ou de révoquer le consentement que vous avez donné. Votre opposition ou votre révocation n'aura d'effet que pour l'avenir. Pour exercer votre droit d'opposition ou de révocation, vous pouvez nous contacter à tout moment à l'adresse suivante : privacy@hornetsecurity.com. Si vous vous opposez au traitement fondé sur notre intérêt légitime, nous pouvons néanmoins poursuivre le traitement si nous pouvons démontrer des motifs légitimes impérieux pour le traitement qui l'emportent sur vos intérêts, droits et libertés.

VII. Droits des personnes concernées

Si des données relatives à votre personne sont traitées, vous êtes la personne concernée au sens de l'article 4, alinéa 1 du RGPD. En tant que personne concernée, vous disposez des droits suivants en ce qui concerne vos données à caractère personnel. Pour exercer ces droits, vous pouvez nous contacter en utilisant les coordonnées indiquées ci-dessus.

Droit d'accès selon l'article 15 du RGPD

Vous avez un droit d'accès à vos données à caractère personnel traitées par nos soins. Cela inclut les informations obligatoires énoncées à l'article 15 du RGPD.

Droit de rectification selon l'article 16 du RGPD

Vous avez le droit d'exiger que les données à caractère personnel erronées soient immédiatement rectifiées et que les données inexactes soient complétées.

Droit à l'effacement selon l'article 17 du RGPD

Vous avez le droit de demander l'effacement de vos données à caractère personnel si l'une des raisons énumérées à l'article 17 du RGPD s'applique, en particulier s'il n'y a plus de base juridique pour le traitement.

Droit à la limitation du traitement selon l'article 18 du RGPD

Vous avez le droit de demander la limitation du traitement de vos données à caractère personnel si l'une des raisons énumérées à l'article 18 du RGPD s'applique, notamment si vous le demandez à la place de l'effacement des données.

Droit à la portabilité des données selon l'article 20 du RGPD

Vous avez le droit de demander toutes les données à caractère personnel que nous avons stockées à votre sujet dans un format structuré, commun et lisible par machine et de transférer ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été fournies ne s'y oppose.

Droit d'introduire une réclamation auprès d'une autorité de contrôle compétente article 77 du RGPD

Conformément à l'article 77 du RGPD, vous avez le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente pour vous.