APPENDICE

ANNEXE I

A. LISTE DES PARTIES

Exportateur(s) de données :

Nom :	Le client qui a conclu l'Accord avec Synology.
Adresse :	L'adresse fournie par le client lorsqu'il s'est inscrit pour utiliser le service C2 de Synology.
Nom, intitulé de poste et coordonnées de la personne à contacter :	Les coordonnées fournies par le Client lorsqu'il s'est inscrit pour utiliser le service C2 de Synology.
Activités relatives aux données transférées en vertu des présentes Clauses :	L'obtention des services C2 fournis par Synology conformément au présent Accord.
Signature et date :	Le présent Accord de protection des données (y compris les Clauses contractuelles standard) sera considéré comme conclu dès l'acceptation de l'Accord par le client.
Rôle :	Contrôleur

Importateur(s) de données :

Nom :	Synology Inc.
Adresse :	9F, No. 1, Yuan Dong Rd., Banqiao, New Taipei 220632, TAÏWAN
Nom, intitulé de poste et coordonnées de la personne à contacter :	L'équipe de protection des données de l'importateur de données peut être contactée comme indiqué dans la Déclaration de confidentialité.
Activités relatives aux données transférées en vertu des présentes Clauses :	La prestation des services C2 fournis au client conformément au présent Accord.
Signature et date :	Le présent Accord de protection des données (y compris les Clauses contractuelles standard) sera considéré comme conclu dès l'acceptation de l'Accord par le client.
Rôle :	Sous-traitant

B. DESCRIPTION DU TRANSFERT

Catégories de personnes concernées dont les données à caractère personnel sont transférées :

Personnes qui passent une commande pour bénéficier des services Synology C2.

Catégories de données à caractère personnel transférées :

Les catégories de données à caractère personnel transférées dépendent de la sélection du Client. Par exemple, le Client peut choisir de sauvegarder des photos, des vidéos et des fichiers personnels sur le service Synology C2.

Données sensibles transférées (le cas échéant) et restrictions ou mesures de protection appliquées qui prennent pleinement en compte la nature des données et les risques encourus, par exemple des limitations strictes concernant la finalité, des restrictions d'accès (y compris autoriser l'accès uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre des accès aux données, des restrictions concernant les transferts ultérieurs ou mesures de sécurité supplémentaires :

Les restrictions et mesures de protection spécifiées dans l'Annexe II s'appliquent à ces catégories de données à caractère personnel (le cas échéant).

La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue) :

Les Données à caractère personnel transférées peuvent être transférées de manière continue jusqu'à ce qu'elles soient supprimées par le client ou conformément au présent Accord.

Nature du traitement :

L'importateur de données traitera les Données à caractère personnel transférées pour stocker, récupérer et transférer ces données conformément au présent Accord.

Finalité(s) du transfert de données et du traitement ultérieur :

Pour l'exécution des services C2 conformément au présent Accord.

La période pendant laquelle les données à caractère personnel seront conservées, ou, si cela n'est pas possible, les critères utilisés pour déterminer cette période :

L'importateur de données conservera les Données à caractère personnel transférées jusqu'à ce qu'elles soient supprimées par le client ou conformément au présent Accord.

Concernant les transferts à destination des sous-traitants/sous-traitants ultérieurs, il est également nécessaire de préciser l'objet, la nature et la durée du traitement :

Voir l'Annexe III

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

L'identification de l'autorité de contrôle compétente doit être établie conformément à la Clause 13.

Commissaire fédéral allemand pour la protection des données et la liberté d'information (BfDI)

ANNEXE II

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS DES MESURES TECHNIQUES ET ORGANISATIONNELLES POUR GARANTIR LA SÉCURITÉ DES DONNÉES

NOTE EXPLICATIVE :

Les mesures techniques et organisationnelles doivent être décrites à l'aide de termes spécifiques (et non génériques). Voir également le commentaire général sur la première page de l'Appendice, en particulier sur la nécessité d'indiquer clairement quelles mesures s'appliquent à chaque transfert/série de transferts.

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toutes les certifications pertinentes) afin de garantir un niveau de sécurité approprié, en tenant compte de la nature, du champ d'application, du contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

1. **Mesures de pseudonymisation et de chiffrement des données à caractère personnel**

Nous utilisons des mesures de pointe pour protéger les données du client.

2. **Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services de traitement**

Nos serveurs, équipements réseau et centres de données offrent une haute disponibilité (HA). Les périphériques matériels tels que les sources d'alimentation, les câbles réseau et les disques système font l'objet de sauvegardes pour éviter que toute défaillance matérielle ne perturbe le fonctionnement des services.

Dans l'infrastructure C2, nous avons développé un codage d'effacement avec une largeur de bande 16+4, stocké sur 20 nœuds de stockage indépendants sur des HDD distincts. Cela signifie que l'objet stocké peut tolérer 4 fragments corrompus au maximum sans que les utilisateurs ne perdent de données. Il est donc peu probable que les pannes matérielles, si elles se produisent, affectent les données C2.

Nous disposons également de deux lignes réseau indépendantes connectées vers l'extérieur. Si une ligne est soumise à une opération de maintenance ou rencontre un problème, notre utilisation ne sera pas affectée, car l'autre ligne continuera à fonctionner.

Nous exploitons certaines mesures telles que le codage d'effacement et la somme de contrôle MD5 pour garantir l'intégrité de nos services C2.

3. **Mesures visant à garantir la possibilité de rétablir rapidement la disponibilité et l'accès aux données à caractère personnel en cas d'incident physique ou technique**

Nos fichiers sont stockés en déployant un code d'effacement, ce qui permet d'effectuer plusieurs copies des données. Cette mesure garantit qu'en cas de panne soudaine de la machine, les données ne seront pas perdues.

En outre, notre base de données sauvegarde régulièrement les données en cas d'anomalies ou d'attaques.

4. **Processus de test et d'évaluation réguliers pour vérifier l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement**

Les services C2 effectuent des analyses de vulnérabilité régulières et tous les problèmes détectés seront rapidement résolus.

Nous surveillons tous les événements d'urgence liés aux produits. Si les produits concernés sont touchés lorsqu'un événement se produit, nous organisons immédiatement des processus de

résolution et programmons des tests d'assurance qualité et l'homologation. L'ensemble du processus est conçu pour être terminé dans les 24 heures suivant le jour où nous avons pris connaissance du problème.

5. **Mesures d'identification et d'autorisation des utilisateurs**

Nos services C2 utilisent le compte Synology pour identifier et autoriser les utilisateurs. Les utilisateurs peuvent se connecter à leurs comptes en saisissant un mot de passe ou via l'authentification à 2 facteurs. S'ils choisissent d'activer l'authentification à 2 facteurs, ils recevront le code de vérification sur leur téléphone portable ou à l'adresse e-mail qu'ils ont associée à leur compte Synology pour s'authentifier lors de la connexion.

6. **Mesures de protection des données pendant la transmission**

Tous nos services C2 utilisent le protocole SSL avec TLS v1.2 pour empêcher toute modification ou corruption des données pendant la transmission. En outre, la plupart de nos services C2 protègent la sécurité de vos données en proposant une C2 Encryption Key (C2 Key) offrant un chiffrement de bout en bout, et les données sont chiffrées avant la transmission. La C2 Encryption Key est un composant essentiel des services C2 de Synology, car elle garantit la protection de vos données sur les serveurs C2.

7. **Mesures de protection des données pendant le stockage**

Les mesures de chiffrement sont appliquées à tous les services C2. Pour connaître la méthode de chiffrement de chaque service C2, reportez-vous au livre blanc du service correspondant pour plus d'informations.

Tous les services C2 utilisent le chiffrement au repos, ce qui signifie que les données stockées sur le HDD sont chiffrées. Pour les services C2 qui offrent un chiffrement de bout en bout, les données sont stockées dans des bases de données ou sur un stockage en mode objet. Étant donné que les données ont déjà été chiffrées côté client, le Serveur ne peut pas accéder au contenu d'origine.

8. **Mesures visant à garantir la sécurité physique des lieux où les données à caractère personnel sont traitées**

Nous utilisons plusieurs mesures de protection physiques, procédurales et technologiques pour protéger vos données et vos systèmes informatiques.

- Sécurité physique : la sécurité commence par la conception et le lieu. Nos centres de données utilisent des protections supplémentaires telles que des clôtures, des sas, des portes verrouillées et des cages pour serveurs.
- Protocoles de sécurité : certaines politiques et procédures sont mises en œuvre pour garantir que les équipes de sécurité et le personnel opérationnel sont disponibles sur site 24h/24, 7j/7 et toute l'année afin de gérer les événements imprévus courants et inhabituels.
- Mesures de protection technologiques : les verrous biométriques sur les portes extérieures, les caméras de vidéosurveillance sur l'ensemble du campus et les points de contrôle des accès sécurisés ne sont que quelques-uns des moyens que nous utilisons pour protéger vos données et votre équipement.

9. **Mesures visant à garantir la journalisation des événements**

Afin de garantir l'accès sécurisé aux services C2, nous disposons d'un processus strict pour réguler et surveiller les connexions externes via les comptes Synology. Nous avons mis en place des mesures de protection contre les menaces potentielles, notamment la détection et le blocage des tentatives de connexion suspectes ou anormales à partir d'adresses IP ou de comptes spécifiques, ainsi que le maintien des autorisations appropriées pour garantir que seuls les utilisateurs autorisés

puissent accéder à nos services.
Synology consigne tous les événements de connexion et d'accès aux données afin de gérer l'identité des utilisateurs. Seuls certains membres de l'équipe ont le droit d'accéder aux systèmes de gestion de la sécurité de l'information.
Les adresses IP dont les tentatives de connexion au VPN ont échoué à plusieurs reprises seront bloquées. Nous envoyons également les rapports de connexion quotidiens aux utilisateurs correspondants et à notre service informatique à des fins d'audit.

10. **Mesures permettant de garantir la configuration du système, y compris la configuration par défaut**

Il n'est possible de se connecter à nos systèmes internes que via une adresse IP intranet. Tous les ports dangereux sur les systèmes sont fermés. Afin de garantir la sécurité et la stabilité du réseau, nous avons mis en place des pare-feu avec détection des anomalies. L'accès à partir d'adresses IP externes n'est pas autorisé, et toutes les demandes et tous les processus d'accès sont étroitement surveillés et enregistrés dans un journal. Si le pare-feu échoue pour une raison inattendue, une alerte est immédiatement déclenchée et enregistrée dans le journal à des fins d'examen et d'optimisation.
Seuls certains membres de l'équipe sont autorisés à accéder aux systèmes de gestion de la sécurité de l'information, et l'accès aux données nécessite de passer par un processus d'authentification.

11. **Mesures pour l'infrastructure informatique interne, et gestion et gouvernance de la sécurité informatique**

Synology impose une politique interne qui oblige tous les employés à utiliser notre TOTP (Time-based One-Time Password) propriétaire pour l'authentification. Cela garantit une sécurité renforcée et réduit le risque d'attaques visant les mots de passe. De plus, les adresses IP dont les tentatives de connexion au VPN ont échoué à plusieurs reprises seront bloquées. Nous envoyons également les rapports de connexion quotidiens aux utilisateurs correspondants et à notre service informatique à des fins d'audit.
Il est obligatoire d'installer un logiciel antivirus et de configurer des pare-feu sur tous nos périphériques professionnels afin de les protéger contre les virus ciblant les fichiers, les e-mails et autre virus Web ou les programmes malveillants. Nous autorisons SPF, DKIM et DMARC à effectuer régulièrement des tests d'hameçonnage par e-mail.
En outre, nous déployons Honeypot dans notre environnement informatique interne. Lorsqu'une activité d'analyse de port est détectée, notre serveur reçoit une notification et bloque l'adresse MAC et le port réseau de l'adresse IP.
Nous proposons également des formations régulières sur la sécurité des informations à notre service informatique.

12. **Mesures pour la certification/l'assurance des processus et des produits**

Tous les logiciels sont développés selon des procédures standard, et la qualité du code est garantie par des révisions de code.
Nous utilisons une procédure pour évaluer la sécurité du code et gérer les logiciels à l'aide de fichiers de configuration à des fins de contrôle.
Des tests seront effectués de bout en bout avant la mise en service de nos logiciels, y compris l'exécution de tests de fumée à l'aide de notre logiciel de test développé en interne.
Nos logiciels sont déployés selon le modèle Canary afin d'en publier progressivement la dernière version et de garantir ainsi leur stabilité.

13. **Mesures pour garantir la minimisation des données**

Synology collecte des informations uniquement pour vous fournir les services C2, et nous ne consultons pas et n'analysons pas les données que vous chargez, sauf pour la sauvegarde du service

cloud. Nous accédons à certaines parties du contenu pour fournir un service et une fonction de recherche avec votre autorisation.
Les utilisateurs peuvent supprimer leurs données à tout moment pendant leur période d'abonnement aux services Synology C2. Une fois que l'abonnement prend fin, toutes les données sont supprimées après la « période de grâce » définie dans les Conditions d'utilisation de Synology C2.
Si les utilisateurs choisissent de supprimer leur compte Synology, leurs données et l'état de leur abonnement C2 seront également invalidés et supprimés.

14. **Mesures pour garantir la qualité des données**

Veuillez vous reporter au point 2 de l'Annexe II.

15. **Mesures pour garantir une conservation limitée des données**

Synology supprime les données qui ne sont plus nécessaires en fonction des spécificités de chaque service.
Les utilisateurs peuvent supprimer leurs données à tout moment pendant la période d'abonnement aux services Synology C2. Une fois que l'abonnement prend fin, toutes les données sont supprimées après une « période de grâce » définie par les Conditions d'utilisation de Synology C2. Si l'utilisateur supprime son compte Synology, ses données et l'état de son abonnement Synology C2 seront également perdus et supprimés. Il est possible que Synology conserve les informations de paiement à des fins financières, y compris, mais sans s'y limiter, pour les déclarations fiscales, les audits et la gestion des inventaires. En outre, Synology conservera également des rapports statistiques et des rapports d'incidents relatifs aux applications, à des fins d'analyse et pour une durée maximale de 14 mois.

16. **Mesures visant à garantir la responsabilité**

Notre système dorsal est accessible uniquement sur autorisation. Les données des services qui utilisent le chiffrement C2 ont été chiffrées par le Client avant d'être chargées sur le Serveur, de sorte que les données stockées dans les services ne puissent pas être lues ou déchiffrées.
Concernant les services qui utilisent le chiffrement C2, les utilisateurs doivent se connecter à leur compte C2 et saisir la bonne clé de chiffrement s'ils souhaitent modifier leurs données.

17. **Mesures garantissant la portabilité et l'effacement des données**

La plupart de nos services C2 garantissent la portabilité des données, facilitant ainsi les conversions multiplateformes ou multiformats.

18. Pour les transferts à destination des sous-traitants/sous-traitants ultérieurs, il faut également décrire les mesures techniques et organisationnelles spécifiques que le sous-traitant/sous-traitant ultérieur doit prendre afin de pouvoir fournir une assistance au responsable du traitement et, pour les transferts provenant d'un sous-traitant vers un sous-traitant ultérieur, à destination de l'exportateur de données

Le paiement de nos services C2 est traité par des sous-traitants tiers, Cherri Tech, Inc (Tappay) et Stripe, Inc., afin de gérer le mode de paiement et les informations de facturation des utilisateurs en toute sécurité. Ces deux sous-traitants ont déployé des mesures suffisantes garantissant la protection des données à caractère personnel et ont acquis une solide réputation en matière de sécurité des informations personnelles.

Reportez-vous au livre blanc de Synology C2 pour plus d'informations.

ANNEXE III

LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Le sous-traitant a autorisé l'utilisation des sous-traitants ultérieurs suivants :

Fournisseur	**Objectif**	**Centre de données**
Firstcolo GmbH	Fournisseur d'infrastructure cloud pour Synology Inc.	Allemagne
Sabey Data Center Solutions LLC	Fournisseur d'infrastructure cloud pour Synology Inc.	États-Unis
Equinix, Inc.	Fournisseur d'infrastructure cloud pour Synology Inc.	États-Unis
Digicentre Co. Ltd.	Fournisseur d'infrastructure cloud pour Synology Inc.	Taïwan
Zayo Group, LLC.	Fournisseur de services Internet pour Synology Inc.	États-Unis
Chunghwa Telecom Company, Ltd.	Fournisseur de services Internet pour Synology Inc.	Taïwan
Deutsche Telekom AG	Fournisseur de services Internet pour Synology Inc.	Allemagne
Stripe, Inc.	Synology utilise Stripe pour gérer les paiements en toute sécurité.	Allemagne/États-Unis
Cherri Tech, Inc.	Synology utilise Tap Pay de Cherri Tech pour gérer les paiements en toute sécurité.	Taïwan
GateWeb Information Co., Ltd.	Synology utilise GateWeb pour gérer les paiements en toute sécurité.	Taïwan
Apple Inc.	Synology utilise la fonctionnalité d'achats intégrés de l'application Apple iOS pour gérer les paiements en toute sécurité. Synology envoie des messages via le service de notification Push Apple	Allemagne/États-Unis/Taïwan
AWS	Synology envoie des e-mails via AWS SES et envoie des notifications via AWS SNS. Les journaux des e-mails et journaux SNS sont également stockés sur AWS CloudWatch et AWS SNS + AWS SQS à des fins de sauvegarde.	Allemagne/États-Unis/Taïwan
Google LLC	Synology envoie des notifications via Firebase Cloud Messaging de Google LLC.	Allemagne/États-Unis/Taïwan

Synology s'engage à mettre régulièrement cette liste à jour pour permettre aux Sous-traitants de rester informés du champ d'application du sous-traitement associé aux services Synology.