ANHANG

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e):

Name:	Der Kunde, der die Vereinbarung mit Synology geschlossen hat.
Anschrift:	Die bei der Registrierung für die Nutzung von Synologys C2-Dienst vom Kunden angegebene Adresse.
Name, Funktion und Kontaktdaten der Kontaktperson:	Die bei der Registrierung für die Nutzung von Synologys C2-Dienst vom Kunden angegebenen Kontaktdaten.
Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind:	Der Erhalt der von Synology gemäß der Vereinbarung bereitgestellten C2-Dienste.
Unterschrift und Datum:	Diese Datenschutzvereinbarung (einschließlich der Standardvertragsklauseln) gilt mit der Annahme der Vereinbarung durch den Kunden als abgeschlossen.
Rolle:	Verantwortlicher

Datenimporteur(e):

Name:	Synology Inc.
Anschrift:	9F, No. 1, Yuan Dong Rd., Banqiao, New Taipei 220632 TAIWAN
Name, Funktion und Kontaktdaten der Kontaktperson:	Das Datenschutzteam des Datenimporteurs kann wie in der Datenschutzerklärung beschrieben kontaktiert werden.

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind:	Die Bereitstellung der C2-Dienste an den Kunden gemäß der Vereinbarung.
Unterschrift und Datum:	Diese Datenschutzvereinbarung (einschließlich der Standardvertragsklauseln) gilt mit der Annahme der Vereinbarung durch den Kunden als abgeschlossen.
Rolle:	Auftragsverarbeiter

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden:

Personen, die Synology C2-Dienste bestellen.

Kategorien der übermittelten personenbezogenen Daten:

Die Kategorien der übertragenen personenbezogenen Daten basieren auf der Auswahl des Kunden. Beispielsweise kann der Kunde auswählen, persönliche Dateien, Fotos und Videos zu den Synology C2-Diensten zu übertragen.

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

Für diese Kategorien personenbezogener Daten (falls vorhanden) gelten die in Anhang II dargelegten Einschränkungen und Garantien.

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden):

Übermittelte personenbezogene Daten können laufend übermittelt werden, bis sie entweder vom Kunden oder gemäß der Vereinbarung gelöscht werden.

Art der Verarbeitung:

Der Datenimporteur verarbeitet übermittelte personenbezogene Daten, um die Daten gemäß der Vereinbarung zu speichern, wiederherzustellen und zu übermitteln.

Zweck(e) der Datenübermittlung und Weiterverarbeitung:

Die Erbringung der C2-Dienste gemäß der Vereinbarung.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer:

Der Datenimporteur bewahrt die übermittelten personenbezogenen Daten auf, bis sie entweder durch den Kunden oder gemäß der Vereinbarung gelöscht werden.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:

Siehe Anhang III

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

ANHANG II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret (nicht allgemein) beschrieben werden. Beachten Sie hierzu bitte auch die allgemeine Erläuterung auf der ersten Seite der Anlage; insbesondere ist klar anzugeben, welche Maßnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten.

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

- **Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten**
  Wir verwenden die neuesten Datensicherheitsmaßnahmen, um Kundendaten zu schützen.
- **Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste**

im Zusammenhang mit der Verarbeitung

Unsere Server, Netzwerkausrüstung und das Rechenzentrum bieten Hochverfügbarkeit (HA). Für Hardwaregeräte wie Netzteile, Netzwerkkabel und Systemlaufwerke gibt es Backups, um sicherzustellen, dass der Ausfall einer Hardware den Betrieb der Dienste nicht unterbricht. Unsere C2-Infrastruktur wurde mit Erasure Coding mit 16+4 Stripe-Layout und Speicherung über 20 unabhängige Speicherknoten auf separaten HDDs eingerichtet. Das bedeutet, das gespeicherte Objekt kann ein Maximum von 4 beschädigten Fragmenten aufweisen, ohne dass Benutzer Daten verlieren. Daher ist es sehr unwahrscheinlich, dass etwaige Hardwareausfälle die C2-Daten beeinträchtigen.

Wir haben außerdem zwei unabhängige Netzwerkleitungen nach außen. Sollte es bei einer Leitung Wartungsarbeiten oder Probleme geben, wird unsere Nutzung davon nicht berührt, da die zweite Leitung weiterhin funktioniert.

Wir nutzen Maßnahmen wie Erasure Coding und MD5-Prüfsumme, um die Integrität unserer C2-Dienste sicherzustellen.

- **Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**

  Unsere Dateien werden mittels Erasure Coding gespeichert, bei dem mehrere Kopien der Daten angefertigt werden. Diese Maßnahme stellt sicher, dass bei einem plötzlichen Hardwareausfall die Daten nicht verloren gehen.

  Außerdem sichert unsere Datenbank die Daten als Schutz vor Datenanomalien oder Angriffen.

- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung**

  Für die C2-Dienste wird regelmäßiges Scanning auf Sicherheitslücken durchgeführt und alle erkannten Probleme werden prompt behoben.

  Wir überwachen alle produktbezogenen Notfälle. Wenn die relevanten Produkte von einem Vorfall betroffen sind, veranlassen wir sofort Lösungen und planen QA-Tests und Veröffentlichung. Das gesamte Verfahren ist mit dem Ziel gestaltet, binnen 24 Stunden ab dem Tag, an dem wir von dem Vorfall Kenntnis erlangen, abgeschlossen zu werden.

- **Maßnahmen zur Identifizierung und Autorisierung der Nutzer**

  Unsere C2-Dienste nutzen das Synology-Konto zur Identifizierung und Autorisierung von Benutzern. Benutzer können sich mittels Eingabe eines Passworts oder 2-Faktor-Authentifizierung bei ihren Konten anmelden.

Wenn Benutzer die 2-Faktor-Authentifizierung aktivieren, erhalten Sie den Verifizierungscode zur Authentifizierung der Anmeldung entweder auf ihrem Mobiltelefon oder an die mit dem Synology-Konto verknüpfte E-Mail-Adresse.

- **Maßnahmen zum Schutz der Daten während der Übermittlung**
  Alle unsere C2-Dienste verwenden das SSL-Protokoll mit TLS v1.2, um zu verhindern, dass Daten währen der Übertragung modifiziert oder beschädigt werden. Außerdem schützen die meisten unserer C2-Dienste Daten durch einen Ende-zu-Ende-C2 Encryption Key (C2 Key) und die Daten werden vor der Übertragung verschlüsselt. Der C2 Encryption Key ist ein essenzieller Bestandteil von Synologys C2-Diensten und gewährleistet, dass Ihre Daten auf den C2-Servern geschützt sind.
- **Maßnahmen zum Schutz der Daten während der Speicherung**
  Für alle C2-Dienste werden Verschlüsselungsmaßnahmen angewendet. Details zur jeweiligen Verschlüsselungsmethode der einzelnen C2-Dienste finden Sie im White Paper des entsprechenden Dienstes.
  Alle C2-Dienste verwenden Verschlüsselung ruhender Daten, d. h. die auf der HDD gespeicherten Daten sind verschlüsselt. Für C2-Dienste, die Ende-zu-Ende-Verschlüsselung anwenden, werden Daten in Datenbanken oder in Objektspeicher gespeichert. Da die Daten bereits clientseitig verschlüsselt wurden, kann serverseitig nicht auf den ursprünglichen Inhalt zugegriffen werden.
- **Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden**
  Wir verwenden mehrere physische, organisatorische und technische Sicherheitsmaßnahmen zum Schutz Ihrer IT-Systeme und Daten.

- Physische Sicherheit: Sicherheit beginnt bei Gebäudedesign und Standort. In unseren Rechenzentren gibt es zusätzliche Sicherheitsmaßnahmen wie Zäune, Schleusen und verschlossene Türen und Serverkästen.
- Sicherheitsprotokolle: Es wurden Richtlinien und Verfahren implementiert, um sicherzustellen, dass Sicherheits- und Betriebspersonal 365 Tage im Jahr rund um die Uhr für alle Eventualitäten vor Ort zur Verfügung steht.
- Technische Sicherheitsmaßnahmen: Biometrische Schlösser an Außentüren, Überwachungskameras auf dem gesamten Gelände und sichere Zugangskontrollen sind nur einige der Maßnahmen, mit denen wir Ihre Daten und Ausrüstung schützen.

- **Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen**
  Um den sicheren Zugriff auf C2-Dienste zu gewährleisten, haben wir ein strenges Verfahren zur Regulierung und Kontrolle externer Zugriffe über

Synology-Konten. Wir haben Maßnahmen zum Schutz vor potenziellen Bedrohungen implementiert, darunter das Erkennen und Blockieren verdächtiger oder auffälliger Anmeldeversuche von bestimmten IP-Adressen oder Konten sowie das Führen korrekter Berechtigungen, um sicherzustellen, dass nur befugte Benutzer auf unsere Dienste zugreifen können.
Zum Management von Benutzeridentitäten werden sämtliche Anmeldungen und Datenzugriffe von Synology protokolliert. Nur bestimmte Teammitglieder sind zum Zugriff auf die Informationssicherheitsmanagementsysteme befugt.
IP-Adressen mit wiederholten fehlgeschlagenen Anmeldeversuchen beim VPN werden blockiert. Wir senden die täglichen Anmeldeaufzeichnungen auch zu Kontrollzwecken sowohl den jeweiligen Benutzern als auch unserer IT-Abteilung.

- **Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration**
  Die Verbindung zu unseren internen Systemen ist nur über Intranet-IP möglich. Alle unsicheren Ports in den Systemen sind geschlossen. Als weitere Maßnahme zur Gewährleistung von Netzwerksicherheit und Stabilität haben wir Firewalls implementiert, die Auffälligkeiten erkennen. Der Zugriff von externen IP-Adressen ist nicht erlaubt und alle Anfragen und Zugriffe werden genau überwacht und in einem Protokoll verzeichnet. Sollte die Firewall unerwartet ausfallen, wird sofort ein Alarm ausgelöst und zur Kontrolle und Optimierung im Protokoll verzeichnet.
  Nur bestimmte Teammitglieder sind zum Zugriff auf die Informationssicherheitsmanagementsysteme befugt und für den Zugriff auf die Daten muss ein Authentifizierungsprozess durchlaufen werden.
- **Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit**
  Synology implementiert eine interne Richtlinie, die von allen Angestellten verlangt, unser selbstentwickeltes zeitbasiertes Einmalpasswort (TOTP) zur Authentifizierung zu verwenden. Dies erhöht die Sicherheit und senkt das Risiko für Passwortangriffe. Darüber hinaus werden IP-Adressen mit wiederholten fehlgeschlagenen Anmeldeversuchen beim VPN blockiert. Wir senden die täglichen Anmeldeaufzeichnungen auch zu Kontrollzwecken sowohl den jeweiligen Benutzern als auch unserer IT-Abteilung.
  Auf all unseren Arbeitsgeräten müssen zum Schutz vor Datei-, E-Mail- und Webviren oder Schadprogrammen Antivirensoftware installiert und Firewalls eingerichtet sein. Wir aktivieren SPF, DKIM und DMARC für

regelmäßige Phishing-E-Mail-Tests.
Außerdem setzen wir in unserer internen IT-Umgebung Honeypot ein. Wenn Portscanning-Aktivitäten erkannt werden, erhält unser Server eine Benachrichtigung und blockiert MAC-Adresse und Netzwerkport der IP-Adresse.
Wir bieten auch regelmäßige Informationssicherheitsschulungen für unsere IT-Abteilung.

- **Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten**
  Sämtliche Software wird gemäß Standardverfahren entwickelt und die Codequalität wird durch Code-Reviews sichergestellt.
  Wir verwenden ein Verfahren zur Bewertung der Code-Sicherheit und managen die Software mit Konfigurationsdateien zur Kontrolle.
  Bevor unsere Software live geht, werden End-to-End-Tests durchgeführt, einschließlich Smoke Tests mit unserer intern entwickelten Testsoftware.
  Unsere Software verwendet Canary Deployment zur schrittweisen Veröffentlichung der neuesten Version, um die Stabilität der Software sicherzustellen.
- **Maßnahmen zur Gewährleistung der Datenminimierung**
  Synology sammelte Daten nur, um Ihnen die C2-Dienste bereitzustellen, und wir greifen nicht auf Ihre hochgeladenen Daten zu und analysieren diese nicht, ausgenommen für die Cloud-Dienst-Sicherung, bei der wir mit Erlaubnis auf Teile der Inhalte zugreifen, um Dienst und Suchfunktion bereitzustellen.
  Benutzer können während des Abonnementzeitraums der Synology C2-Dienste ihre Daten jederzeit löschen. Wenn der Abonnementzeitraum endet, werden alle Daten nach der in den Synology C2 Nutzungsbedingungen definierten „Nachfrist “ gelöscht.
  Wenn Benutzer ihr Synology-Konto löschen, werden auch ihre Daten und ihr C2-Abonnementstatus ungültig und entfernt.
- **Maßnahmen zur Gewährleistung der Datenqualität**
  Siehe Punkt 2 in Anhang II.
- **Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung**
  Synology löscht nicht mehr benötigte Daten abhängig von den Spezifikationen der einzelnen Dienste.
  Benutzer können während des Abonnementzeitraums der Synology C2-Dienste ihre Daten jederzeit löschen. Wenn das Abonnement endet, werden alle Daten nach einer von den Synology C2 Nutzungsbedingungen definierten „Nachfrist “ gelöscht. Wenn Benutzer

ihr Synology-Konto löschen, werden auch ihre Daten und ihr C2-Abonnementstatus ungültig und entfernt. Synology kann Zahlungsdaten für finanzielle Zwecke wie unter anderem steuerliche Meldung, Wirtschaftsprüfung, Bestandsmanagement aufbewahren. Außerdem bewahrt Synology statistische Berichte und Absturzberichte der Anwendungen zu Analysezwecken maximal 14 Monate lang auf.

- **Maßnahmen zur Gewährleistung der Rechenschaftspflicht**
  Auf unsere Back-End-Systeme kann nur mit Genehmigung zugegriffen werden. Die Daten der Dienste, die C2-Verschlüsselung nutzen, werden vor dem Hochladen zum Server vom Client verschlüsselt, sodass die in den Diensten gespeicherten Daten nicht gelesen oder entschlüsselt werden können.
  Für die Dienste, die C2-Verschlüsselung nutzen, müssen sich Benutzer bei ihrem C2-Konto anmelden und den korrekten Verschlüsselungsschlüssel eingeben, um ihre Daten zu bearbeiten.
- **Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung**
  Die meisten unserer C2-Dienste erlauben Datenübertragbarkeit durch plattform- oder formatübergreifende Konvertierungen.
- **Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.**

Bei der Bezahlung unserer C2-Dienste werden zur sicheren Handhabung der Zahlungsmethoden und Rechnungsdaten von Benutzern die Drittverarbeiter Cherri Tech, Inc. (Tappay) und Stripe, Inc. in Anspruch genommen. Beide Verarbeiter haben angemessene Maßnahmen zum Schutz personenbezogener Daten und haben sich einen guten Ruf hinsichtlich der Gewährleistung der Sicherheit personenbezogener Daten erworben.

Weitere Informationen finden Sie im Synology C2 White Paper.

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme der folgenden Unterauftragsverarbeiter erlaubt:

Anbieter	**Zweck**	**Rechenzentren**

Firstcolo GmbH	Anbieter von Cloud-Infrastruktur für Synology Inc.	Deutschland
Sabey Data Center Solutions LLC	Anbieter von Cloud-Infrastruktur für Synology Inc.	USA
Equinix, Inc.	Anbieter von Cloud-Infrastruktur für Synology Inc.	USA
Digicentre Co. Ltd.	Anbieter von Cloud-Infrastruktur für Synology Inc.	Taiwan
Zayo Group, LLC.	Internetdienstanbieter für Synology Inc.	USA
Chunghwa Telecom Company, Ltd.	Internetdienstanbieter für Synology Inc.	Taiwan
Deutsche Telekom AG	Internetdienstanbieter für Synology Inc.	Deutschland
Stripe, Inc.	Synology verwendet Stripe für die sichere Zahlungsabwicklung.	Deutschland/USA
Cherri Tech, Inc.	Synology verwendet Cherri Techs Tap Pay für die sichere Zahlungsabwicklung.	Taiwan
GateWeb Information Co., Ltd.	Synology verwendet GateWeb für die sichere Zahlungsabwicklung.	Taiwan
Apple Inc.	Synology verwendet In-App-Käufe in Apple iOS für die sichere Zahlungsabwicklung. Synology verschickt Nachrichten via Apple Push-Benachrichtigungsdienst	Deutschland/USA/Taiwan
AWS	Synology verschickt E-Mails via AWS SES und Benachrichtigungen via AWS SNS. E-Mail- und SNS-Protokolle werden außerdem zu Sicherungszwecken in AWS CloudWatch und AWS SNS + AWS SQS gespeichert.	Deutschland/USA/Taiwan
Google LLC	Synology verschickt Benachrichtigungen via Google LLCs Firebase Cloud Messaging.	Deutschland/USA/Taiwan

Synology verpflichtet sich, diese Liste regelmäßig zu aktualisieren, damit Verantwortliche über das Ausmaß der Unterauftragsverarbeitung im Zusammenhang mit Synology-Diensten auf dem Laufenden bleiben können.