APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:	The Customer that has entered the Agreement with Synology.
Address:	The address that the Customer provided when registering to use Synology's C2 service.
Contact person's name, position and contact details:	The contact details that the Customer provided when registering to use Synology's C2 service.
Activities relevant to the data transferred under these Clauses:	The receipt of C2 services provided by Synology pursuant to the Agreement.
Signature and date:	This Data Protection Agreement (including Standard Contractual Clauses) shall be deemed executed upon the Customer's acceptance of the Agreement.
Role:	Controller

Data importer(s):

Name:	Synology Inc.
Address:	9F, No. 1, Yuan Dong Rd., Banqiao, New Taipei 220632 TAIWAN
Contact person's name, position and contact details:	The data importer's data protection team can be contacted as described in the Privacy Statement.
Activities relevant to the data transferred under these Clauses:	The provision of C2 services to the Customer pursuant to the Agreement.
Signature and date:	This Data Protection Agreement (including Standard Contractual Clauses) shall be deemed executed upon the Customer's acceptance of the Agreement.
Role:	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Individuals who order Synology C2 services.

Categories of personal data transferred:

The categories of personal data transferred are based upon the Customer's selection. For instance, the Customer may opt to back up personal files, photographs, videos to Synology C2 service.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

The restrictions and safeguards specified in Annex II apply to these categories of personal data (if any).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Transferred Personal Data may be transferred on a continuous basis until it is either deleted by the customer or in accordance with the Agreement.

Nature of the processing:

The data importer will process Transferred Personal Data to store, recovery, transferring the data in accordance with the Agreement.

Purpose(s) of the data transfer and further processing:

To the performance of the C2 services in accordance with the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The data importer will retain Transferred Personal Data until it is either deleted by the customer or pursuant to the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

See Annex III

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority shall be determined in accordance with Clause 13.

German Federal Commissioner for Data Protection and Freedom of Information (BfDI)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Measures of pseudonymisation and encryption of personal data**
   We employ cutting-edge data protection measures to safeguard the customer's data.
2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**
   Our servers, network equipment, and the data center provide High Availability (HA). Hardware devices such as power suppliers, network cables, and system disks have backups to ensure that a single hardware failure will not disrupt the operation of the services.
   In the C2 infrastructure, we have designed erasure coding with a 16+4 stripe layout and is stored across 20 independent storage nodes on separate HDDs. This means that the stored object can tolerate a maximum of 4 corrupted fragments without users losing data. Hardware-level failures, if they occur, are thus highly unlikely to affect C2 data.
   We also have two independent network lines to the outside. In case one line undergoes maintenance or encounters an issue, our usage will remain unaffected as the other line continues to operate.
   We utilize measures such as erasure coding and MD5 checksum to ensure the integrity of our C2 services.
3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**
   Our files are stored by adopting erasure coding, which makes multiple copies of data. This measure ensures that in the event of a sudden machine failure, the data will not be lost.
   In addition, our database will back up the data regularly in case of data abnormalities or attacks.
4. **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**
   C2 services conduct regular vulnerability scanning, and any detected issues will be promptly resolved.
   We monitor all product-related emergency events. If the relevant products are affected when an event occurs, we will immediately arrange for resolutions and schedule QA testing and release. The entire process is designed to be completed within 24 hours from the day we become aware of the issue.
5. **Measures for user identification and authorisation**
   Our C2 services use Synology Account for user identification and authorisation. Users can

log into their accounts either by entering a password or through 2-factor authentication. If users choose to enable 2-factor authentication, they will receive the verification code either on their mobile phone or have it sent to their email associated with Synology Account for login authentication.

6. **Measures for the protection of data during transmission**
   All of our C2 services utilize the SSL protocol with TLS v1.2 to prevent data from being modified or corrupted during transmission. Additionally, most of our C2 services protect data security by adopting end to end C2 Encryption Key (C2 Key), and the data is encrypted before the transmission. The C2 Encryption Key is a critical component of Synology's C2 services, ensuring that your data remains protected in C2 servers.
7. **Measures for the protection of data during storage**
   Encryption measures are applied to all C2 services. For each C2 service's encryption method, please refer to the corresponding service white paper for further details.
   All C2 services use encryption-at-rest, which means that the data stored on the HDD is encrypted. For C2 services that adopt end to end encryption, data is stored within databases or stored on object storage. Since the data has already been encrypted on the Client end, the Server end is unable to access the original content.
8. **Measures for ensuring physical security of locations at which personal data are processed**
   We use multiple physical, procedural, and technological safeguards to safely protect your IT systems and data.
   - Physical Security: Security starts with building design and location. Our data centers utilize additional protections such as fences, mantraps, and locked doors and server cages.
   - Security Protocols: Policies and procedures are implemented to ensure that security personnel and operations staff are available onsite 24×7×365 to handle both common and unusual contingencies.
   - Technological Safeguards: Biometric locks on outside doors, CCTV cameras throughout the campus, and secure access checkpoints are just a few of the ways we protect your data and equipment.
9. **Measures for ensuring events logging**
   To ensure the secure access of C2 services, we have a strict process for regulating and monitoring external logins through Synology Accounts. We have implemented measures to protect against potential threats, including detecting and blocking suspicious or abnormal login attempts from specific IP addresses or accounts, as well as maintaining proper permissions to ensure that only authorized users can access our services.
   Synology logs all login and data access events to manage user identity. Only specific team members have the authority to access the information security management systems.
   IP addresses with repeated unsuccessful login attempts to the VPN will be blocked. We also send the daily login records to both the respective users and our IT department for auditing purpose.
10. **Measures for ensuring system configuration, including default configuration**
    Our internal systems can only be connected through intranet IP. All the unsafe ports on the systems are closed. To further ensure network security and stability, we have implemented firewalls with anomaly detection. Access from external IP addresses is not permitted, and all requests and access processes are closely monitored and recorded in a log. If the firewall

fails for any unexpected reason, an alert will be immediately triggered and recorded in the log for review and optimization.

Only specific team members have the authority to access the information security management systems, and accessing the data requires going through an authentication process.

11. **Measures for internal IT and IT security governance and management**

Synology implements an internal policy that requires all employees to use our self-developed TOTP (Time-based One-Time Password) for authentication. This ensures enhanced security and reduces the risk of password attacks. Additionally, IP addresses with repeated unsuccessful login attempts to the VPN will be blocked. We also send the daily login records to both the respective users and our IT department for auditing purpose.

All our devices for work are required to install antivirus software and set up firewalls to protect against file, email, and web viruses or malicious programs. We enable SPF, DKIM, and DMARC to regularly conduct phishing email tests.

In addition, we deploy Honeypot in our internal IT environment. When any port scanning activity is detected, our server will receive a notification and proceed to block the MAC address and network port of the IP address.

We also provide regular training on information security for our IT department.

12. **Measures for certification/assurance of processes and products**

All software is developed following standard procedures, and the code quality is ensured through code reviews.

We use a procedure to evaluate code security and manage the software using configuration files for control.

End-to-end testing will be conducted before our software goes live, including the execution of smoke tests using our internally developed testing software.

Our software adopts canary deployment to gradually release the latest version for ensuring software stability.

13. **Measures for ensuring data minimisation**

Synology collects information only to provide you with the C2 services, and we do not access or analyze the data you upload, except for the cloud service backup, we will access parts of the content to provide service and search feature with permission.

Users can delete their data at any time during the subscription period of Synology C2 services. Once the subscription period ends, all the data will be deleted after the "grace period" defined in the Synology C2 Terms of Service.

If users choose to delete their Synology Account, their data and C2 subscription status will also be invalidated and removed.

14. **Measures for ensuring data quality**

Please refer to point 2 of Annex II.

15. **Measures for ensuring limited data retention**

Synology will delete the data that is no longer needed depending on the specifics of each service.

Users can delete their data anytime during the subscription period of Synology C2 services. Once the subscription ends, all the data will be deleted after a "grace period" defined by the Synology C2 Terms of Service. If user delete their Synology Account, the data and subscription status for Synology C2 will also be forfeited and removed. Synology may retain payment information for financial purposes, including but not limited to tax reporting,

auditing, and inventory management. Additionally, Synology will also retain statistical reports and crash reports of the applications for analysis purposes for a maximum of 14 months.

16. **Measures for ensuring accountability**
    Our back-end system can only be accessed with permission. The data of the services that utilize C2 encryption have been encrypted by Client before being uploaded to Server, so the data stored in the services is unable to be read or decrypted.
    For the services that utilize C2 encryption, users need to log in to their C2 account and enter the correct encryption key if they would like to edit their data.
17. **Measures for allowing data portability and ensuring erasure**
    Most of our C2 services allow data portability, enabling cross-platform or format conversions.
18. **For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

The payment of our C2 services use the third-party processors, Cherri Tech, Inc. (Tappay) and Stripe, Inc., to securely handle users' payment method and billing information. Both of the processors have sufficient measures to safeguard personal data, and have earned a strong reputation for ensuring the safety of personal information.

Please refer to Synology C2 white paper for more information.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Vendor	**Purpose**	**Data Centers**
Firstcolo GmbH	Cloud infrastructure provider for Synology Inc.	Germany
Sabey Data Center Solutions LLC	Cloud infrastructure provider for Synology Inc.	USA
Equinix, Inc.	Cloud infrastructure provider for Synology Inc.	USA
Digicentre Co. Ltd.	Cloud infrastructure provider for Synology Inc.	Taiwan
Zayo Group, LLC.	Internet service provider for Synology Inc.	USA
Chunghwa Telecom Company, Ltd.	Internet service provider for Synology Inc.	Taiwan
Deutsche Telekom AG	Internet service provider for Synology Inc.	Germany
Stripe, Inc.	Synology uses Stripe to securely handle payment.	Germany/ USA
Cherri Tech, Inc.	Synology uses Cherri Tech's Tap Pay to securely handle payment.	Taiwan
GateWeb Information Co., Ltd.	Synology uses GateWeb to securely handle payment.	Taiwan
Apple Inc.	Synology uses Apple iOS in-app purchase to securely handle payment. Synology sends messages via Apple Push Notification Service	Germany/ USA/Taiwan
AWS	Synology sends Email via AWS SES, and send notifications via AWS SNS. Email and SNS logs are also stored at AWS CloudWatch and AWS SNS + AWS SQS for backup purpose.	Germany/ USA/Taiwan
Google LLC	Synology sends notifications via Google LLC's Firebase Cloud Messaging.	Germany/ USA/Taiwan

Synology commits to keep this list updated regularly, to enable Controllers stay informed of the scope of sub-processing associated with Synology services.