Data Processing Agreement

between

Customer

(Hereinafter referred to as "the Controller")

and

Synology

(Hereinafter referred to as "the Processor").

1. Definitions

Agreement means this Data Processing Agreement.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Cross-border processing means either:

1. processing of Personal Data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

2. processing of Personal Data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data Protection Officer means an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data Subject means a natural person whose Personal Data is processed by a controller or

processor.

Encrypted Data means Personal Data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

GDPR means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Privacy by Design means a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Privacy Impact Assessment means a tool used to identify and reduce the privacy risks of entities by analysing the Personal Data that are processed and the policies in place to protect the data.

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

Profiling means any automated processing of Personal Data intended to evaluate, analyse, or predict data subject behavior.

Pseudonymisation means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Recipient means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under the GDPR.

Reseller means a third-party service provider who subscribe Synology C2 service and pay the remuneration of such service directly to the Processor on behalf of the Controller.

Regulations mean the GDPR and other generally binding legal regulations relating to the area of Personal Data protection.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 GDPR.

2. Subject matter and Duration of the Agreement

(1) Subject matter

The subject-matter of this Agreement is derived from the Synology C2 Service Agreement available at https://c2.synology.com/en-global/legal/terms_conditions (hereinafter referred to as "Service Agreement").

(2) Duration

The duration of this Agreement corresponds to the duration of the Service Agreement.

3. Nature and Purpose of the Agreement

(1) Nature and Purpose of the intended Processing of Data

The nature and purpose of the processing of Personal Data by the Processor for the Controller are precisely defined in the Service Agreement.

(2) Type of Data

The Subject Matter of the processing of Personal Data comprises the following data types/categories:

- Personal Main Data: The controller may store data of any kind on the rented server at his own discretion. Synology has no influence and no access on this.
- Contract Billing and Payments Data: Within the framework of the execution of the Synology C2 Service Agreement, Synology shall collect the personal contractual data including contact address, information on the payment method, contact person.

(3) Categories of Data Subjects

The Categories of Data Subjects comprise of Customers and Contact Persons of the Resellers.

4. Obligations of the Processor

(1) The Processor processes Personal Data solely and in full compliance with the Regulations and instructions of the Controller or as otherwise required in this Agreement. This obligation also applies to transfers by the Processor of Personal Data to a third country or an international organisation, unless the Processor is required to do so by the Regulations or laws to which the Processor is subject. In such a case, the Processor shall inform the Controller of such legal requirements before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Processor and Controller agree that this Agreement and the Synology C2 Service Agreement represents the Controller's complete and final instructions to the Processor. Processing outside the scope of this Agreement (if any) will require prior written agreement between both parties on additional instructions for processing. The Controller may terminate this Agreement if the Processor declines to follow instructions requested by the Controller that are outside the scope of this Agreement.

(3) In the performance of this Agreement, the Controller shall immediately confirm any oral instructions in writing.

(4) Copies or duplicates of the data processed on behalf of the Controller shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data under the Regulations.

(5) The Processor may not on its own authority rectify, erase, or restrict the processing of data that is being processed on behalf of the Controller or port/transfer any such data to any third party, but do so only on documented instructions from the Controller. When a Data Subject contacts the Processor directly concerning a rectification, erasure, or restriction of processing or to exercise the right of portability, the Processor will immediately forward the Data Subject's request to the Controller. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Processor in accordance with documented instructions from the Controller without undue delay.

(6) The Processor shall inform the Controller immediately if the Processor considers that an instruction of the Controller violates the GDPR (with regard to Art. 28 Paragraph 3 Sentence 3) or the Regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

(7) In addition to complying with the rules set out in this Agreement, the Processor shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR. Accordingly, the Processor assures particularly compliance with the following requirements:

a) The Processor entrusts only such employees with the data processing outlined in this Agreement who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Processor and any person acting under its authority who has access to Personal Data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this

Agreement, unless required to do so by law (Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR).

b) The Processor must assist the Controller to comply with requests from individuals exercising their rights to access, rectify, port, erase or object to the processing of their Personal Data.

c) The Processor must assist the Controller to comply with requests from the supervisory authority. The Controller and the Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.

d) Designation of Data Protection Officer / Contact Person / Representative

Synology's Data Protection Team can be contacted at https://www.synology.com/en-global/form/privacy_issue. The Controller shall be informed immediately of any change of Data Protection Officer.

e) The Controller shall be informed immediately of any inspections and measures conducted by the relevant supervisory authority as described in Point 9 of this Agreement, insofar as they relate to the processing of this Agreement.

f) Insofar as the Controller is subject to an inspection by a supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Agreement data processing by the Processor, the Processor shall make every effort to support the Controller. Further assistance duties are described in Point 8 of this Agreement.

g) The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 as described in Point 9 of this Agreement.

h) Implementation of and compliance with all Technical and Organisational Measures necessary for this Agreement in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR, as detailed in the Appendix.

5. Notification duties

(1) The Processor shall immediately notify the Controller of any Personal Data breaches. Any justifiably suspected incidences are also to be reported. Any notification must, at the very least, contain the information provided for in Art. 33 section 3 of the GDPR.

(2) The Controller must also be notified immediately of any significant disruptions when carrying out the task as well as violations against the legal data protection provisions or the stipulations in this Agreement carried out by the Processor or any individuals he/she employs.

(3) The Processor shall immediately inform the Controller of any inspections or measures carried out by supervisory authorities or other third parties if they relate to the commissioned data processing.

(4) The Processor shall ensure that the Controller is supported in these obligations, in accordance with Art. 33 and Art. 34 of the GDPR, to the extent required.

6. Technical and Organisational Measures & Data Security

(1) Before the commencement of processing and prior to conclusion of the Agreement, the Processor shall implement and comply with the technical and organisational measures ("Technical and Organizational Measures") in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR

in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that ensuring an appropriate level of protection achieved by Technical and Organizational Measures. The measures take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events. The measures to be taken shall guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account.

(2) The Technical and Organisational Measures are subject to technical progress and further development. Therefore the Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of the Regulations and the protection of the rights of the data subject. In this respect, the Processor is obligated to implement current state of the art or substitute adequate measures. Substantial changes must be documented.

(3) The Technical and Organizational Measures are described in detail in Appendix 1 of this Agreement

7. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as services which relate directly to the provision of the principal service. This does not include subsidiary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced subsidiary services.

(2) The Processor may authorize subcontractors only after prior explicit written or documented consent from the Controller. Notwithstanding the aforementioned, the Controller shall not withhold its consent without objectively justified reasons.

(3) Outsourcing to subcontractors or changing the existing subcontractor are permissible when:

- The Processor submits such an outsourcing to a subcontractor to the Controller in writing or in text form with appropriate advance notice; and
- the Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Processor; and
- the same data protection obligations as set out in this Agreement shall be imposed on that other processor (subcontractor) by way of a contract/agreement or the subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(4) The Processor will impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this Agreement or the legal requirements set out by the GDPR,

including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights.

(5) The transfer of Personal Data from the Controller to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after all compliance requirements has been achieved.

(6) The Processor will restrict the subcontractor's access to the data only to what is necessary to maintain the service of the subcontractor and will prohibit the subcontractor from accessing data for any other purpose.

(7) The Processor will remain responsible for its compliance with the obligations of this Agreement and for any acts or omissions of the subcontractor that cause the Processor to breach any of Processor's obligations under this Agreement.

(8) If the subcontractor provides the agreed service outside the EU/EEA, the Processor must ensure compliance with the Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2 of the GDPR.

(9) Further outsourcing by the subcontractor requires the express consent of the Processor (at the minimum in text form); all contractual provisions in this Agreement shall be communicated to and agreed with each and every additional subcontractor.

8. Obligations, Rights and Supervisory of the Controller

(1) The Controller shall be solely responsible for assessing the admissibility of the processing requested and for the rights of affected parties.

(2) The Controller has the right to carry out inspections on the Processor or to have them carried out by an auditor to be designated in each individual case. The Controller has the right to check the compliance with this Agreement by the Processor in its business operation times by means of random checks, which are ordinarily to be announced in reasonable time.

(3) Inspections at the Processor's premises must be carried out without any avoidable disturbances to the operation of Processor's business. Unless otherwise indicated for urgent reasons, which must be documented by the Controller, inspections shall be carried out after appropriate advance notice and during the Processor's business hours, and not more frequently than every 12 months. If the Processor provides evidence of the agreed data protection obligations being correctly implemented, as stipulated in chapter 5 (8) of this Agreement, any inspections shall be limited to samples.

(4) The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with Article 28 GDPR. The Processor undertakes to give the Controller the necessary information on request, to demonstrate the execution of the Technical and Organizational Measures.

(5) Evidence of such measures, which concern not only this Agreement, may be provided by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor).

(6) The Processor may claim remuneration for enabling Controller inspections.

9. Assistance and Information Duties of the Processor

(1) The Processor shall assist the Controller in complying with the obligations concerning the security of Personal Data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a. Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b. The obligation to report a Personal Data breach immediately to the Controller.

c. The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.

d. The duty to assist the Controller with regard to the Controller's obligation to provide information to the supervisory authority. The Controller shall cooperate, on request, with the supervisory authority in performance of its tasks.

e. Supporting the Controller with its data protection impact assessment.

f. Supporting the Controller with regard to prior consultation of the supervisory authority.

(2) The Controller shall be informed immediately of any inspections and measures conducted by a supervisory authority, insofar as they relate to the processing of data related to this Agreement. This also applies insofar as the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any law or administrative rule or the Regulations regarding the processing of data in connection with the processing of this Agreement. Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the data processing by the Processor under this Agreement, the Processor shall make every effort to support the Controller and provide all documentation, resources, and support as the Controller may require. Where data concerning this Agreement becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by the Processor, the Processor will inform the Controller without undue delay. The Processor will, without undue delay, notify and update the Controller without undue delay of all developments and updates in such actions, and shall take all measures in response to such actions as required by the Controller.

(3) The Processor may claim compensation for support services which are not included in the description of the services hereof and which are not attributable to failures of the Processor, provided that such compensation are approved in advance in writing by the Controller.

10. Remuneration

The Processor's remuneration for its services rendered under this Agreement is conclusively stipulated in the Service Agreement. There is no separate remuneration or reimbursement provided in this Agreement].

11. Liability and Indemnification

(1) The Controller and the Processor shall be respectively liable for damages caused by any unauthorised party or for incorrect data processing within the scope of this Agreement in accordance with the applicable laws.

(2) The Processor shall bear the burden for proving that any damage is not the result of circumstances that the Processor is responsible for insofar as the relevant data have been processed under this Agreement. If this proof has not been provided, the Processor shall, when initially requested to do so, release the Controller from all claims that are levied against the latter in connection with the data processing under this Agreement.

(3) The Processor shall be liable to the Controller, shall fully indemnify the Controller for all direct damages sustained by the Controller, and shall hold the Controller harmless, for any and all direct damages caused by the Processor, the Processor's employees or appointed subcontractors, in connection with rendering of services by the Processor under this Agreement.

(4) In no event shall either party be liable to the other for any indirect, punitive, special, incidental, or consequential damages in connection with or related to this agreement (including loss of profits, use, data, or other economic advantage), however arising, whether for breach of this agreement, including breach of warranty or in tort, even if that party has been previously advised of the possibility of such damage.

(5) Sections 11 (2) and 11 (3) shall not apply to the extent that the damages occurred as a result of the Processor correctly implementing the services in the manner requested or instructed by the Controller.

12. Right to extraordinary termination

(1) The Controller may, at any time, terminate the Service Agreement and/or this Agreement without notice ('extraordinary termination') if a serious infringement of the Regulations or the provisions of this Agreement exists on part of the Processor, if the Processor cannot or will not execute the Controller's legal instructions or if the Processor refuses to accept the Controller's supervisory rights, in violation of this Agreement.

(2) A serious breach shall, in particular, be deemed to have occurred if the Processor has not substantially fulfilled or failed to fulfil the obligations laid down in this Agreement, in particular the technical and organisational measures.

(3) For insignificant breaches, the Controller shall provide the Processor with a reasonable period of time, not to exceed thirty (30) days, to remedy the situation. Should the situation not be remedied in such period of time, the Controller shall be entitled to extraordinary termination as stipulated here.

13. Termination, Return and Deletion of data

(1) After termination of this Agreement or the termination of the underlying Service Agreement or upon request by the Controller, the Processor shall hand over to the Controller or – subject to prior consent of the Controller – destroy all data, processing and utilization results and data sets related

to this Agreement or Service Agreement that have come into the Processor's possession, in a data-protection compliant manner in compliance with the Regulations. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided to the Controller upon completion of the destruction or deletion or at any time as requested by the Controller.

(2) Documentation which is used to demonstrate orderly data processing in accordance with this Agreement shall be stored by the Processor beyond the duration of this Agreement in accordance with the respective retention periods under the Regulations. The Processor may hand such documentation over to the Controller at the end of the duration of this Agreement or at any time as requested by the Controller.

(3) The Processor is obligated to immediately ensure the return or deletion of data from subcontractors.

(4) The Processor must provide proof of the data being properly destroyed by the Processor or subcontractors and immediately submit this proof to the Controller.

14. Miscellaneous

(1) Both Parties are obligated to treat all knowledge of trade secrets and data security measures, which have been obtained by the other party within the scope of the contractual relationship, confidentially, even after this Agreement has expired. If there is any doubt as to whether information is subject to confidentiality, it shall be treated confidentially until written approval from the other party has been received. No ownership interest in intellectual property rights shall pass from the Controller to the Processor under this Agreement.

(2) Any amendments to this Agreement shall be in writing and be agreed by both Parties.

(3) Any exemption to the right of retention under applicable laws is hereby ruled out with regard to the data processed and the associated data carriers.

(4) Should any parts of this Agreement be invalid, this will not affect the validity of the remainder of this Agreement.

(5) This Agreement shall be governed by and construed in accordance with the laws of [the country where Processor located], without regard to that body of law controlling conflicts of law.

(6) All disputes arising out of or in connection with this Agreement shall fall within the jurisdiction of the Federal Republic of Germany subject to the obligations of international private law, excluding the UN Convention on Contracts for the International Sale of Goods.
If the client is a merchant according to § 1 paragraph 1 of the German Commercial Code (HGB), a legal entity of public law or an special fund of public law, the courts in Düsseldorf have jurisdiction over any disputes arising from or in connection with this contractual relationship.

Appendix - Technical and Organisational Measures

1. **Confidentiality (Article 32 Paragraph 1 Point b GDPR)**

- No unauthorised access Physical Access Control
  to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
  No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Controller support, sandboxing;
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of Personal Data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. **Integrity (Article 32 Paragraph 1 Point b GDPR)**

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- Data Entry Control
  Verification, whether and by whom Personal Data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. **Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**

- Availability Control
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. **Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third party data processing as per Article 28 GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.