

Pre-contractual information Disclosure (for Connected Products and Related Services)

This Pre-Contractual Information Disclosure (the “Disclosure”) sets out the information required under Regulation (EU) 2023/2854 (the “EU Data Act”) in relation to Synology Inc.’s connected products and related services (collectively, the “Products and Services”).

This Disclosure describes the data generated through the use of the Products and Services, including the general nature of such data, the purposes for which it may be used, and the conditions under which access to or sharing of such data may occur.

1. Products and Services

This Disclosure applies to the following categories of Products and Services:

- **Connected Products**
Synology network-connected hardware devices, including:
 - NAS systems
 - Routers
 - Cameras
 - BeeStation devices
 - Active Protect DP series
 - NVR series
- **Related Services**
Services integrated with or supporting the operation, management, monitoring, maintenance, updating, or support of the connected products, including:
 - Active Insight
 - BeeStation Portal

The specific data generated depends on the product model, firmware or software version, enabled features, configuration settings, and any related services used together with the connected product.

2. Data Generated by Use of The Product and Service

The Products and Services may generate data as a result of their operation, configuration, and user interaction. Such data may include:

- System operational data, including information relating to device status and system functionality;
- System logs, including diagnostic records and event logs;
- User access logs, reflecting authentication and administrative activities;
- Performance metrics, relating to system performance and resource utilization; and
- Application or service usage data, reflecting feature activation and interaction with device or service functionality.

In addition, the BeeStation Portal, as a related service, may generate certain service-specific data associated with user accounts and service interaction, including user identifiers, basic profile information, and usage and activity metadata.

3. Data Format, Volume, and Generation Characteristics

3.1. Data Format

Data may be recorded and processed in formats including IETF- and BSD-based formats, plain text, HTML, CSV, JSON, log files, compressed files (e.g. .gz, .xz), database files (e.g. .db, .sqlite), or other formats determined by the technical design of the relevant Product or Service.

3.2. Data Volume

Data volumes may vary depending on configuration, workload intensity, enabled features, and usage patterns, and may range from kilobytes (KBs) to megabytes (MBs) or gigabytes (GBs).

3.3. Data Generation Frequency

Data may be generated continuously, in near real time, or on an event-driven basis, depending on the technical design and configuration of the relevant Product or Service.

4. Data Storage, Retention, and User Access

4.1. Data Storage Location

Data generated by the Connected Products is stored locally on the device. Depending on product configuration, enabled features, and associated services, certain data may also be stored or transmitted to a remote server, such as another Synology device or Synology C2 Cloud, where applicable. For Related Services, data is generally stored on remote servers operated by or on behalf of Synology, including Synology C2 Cloud and the BeeCloud server, in order to enable service functionality, monitoring, or user access.

4.2. Intended Duration of Retention

Retention of data generated by Connected Products generally depends on user configuration and storage capacity.

For certain Related Services, retention periods may be defined by service design or contractual terms, such as for a specified period following collection or for as long as the user maintains an active account. Retention may also be influenced by applicable legal obligations.

4.3. User Access, Retrieval, and Erasure

Users may access, export, or delete data generated by the Products and Services through available user interfaces, management tools, or service portals, subject to technical feasibility and applicable permissions. Where direct access is not

available, users may submit requests by contacting Synology, which will be handled in accordance with applicable legal and contractual requirements.

4.4. Technical Means

Technical means include HTTPS, SSH, standard file-service protocols(SMB, NFS), or RESTful APIs, depending on the specific Product or Service and its technical design.

5. Data Sharing

Data generated by the Products and Services may be shared with third parties only where necessary for the provision, operation, support, maintenance, or improvement of the Products and Services, or where required by applicable law. Such third parties may include service providers or partners acting on behalf of Synology. Appropriate safeguards are applied to protect data security and confidentiality.

Access to data may be restricted where strictly necessary to protect trade secrets, intellectual property rights, system security, or other legitimate interests permitted under the EU Data Act.

6. Contact

For questions regarding this Disclosure or to exercise data access rights under the EU Data Act, users may contact Synology through their Synology Account, submit a request via the [online form](#) available on our website, or contact: Synology Inc., 9F, No. 1, Yuan Dong Rd., Banqiao, New Taipei 220632, TAIWAN.