EU Data Act Compliance for Security Camera (Version 1.0)

EU Data Act Compliance Document (Security Camera Category)-EN

EU Data Act Transparency Statement (Security Camera / DVR Kits)

I. Scope of Application

1. Applicable Product Types: DVR, POE NVR, Wireless NVR, Wi-Fi Camera
2. Applicable Markets: All EU Member States (including Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden)
3. Document Languages: English, German, French, Italian, Spanish, Dutch
4. Applicable Regulations: Regulation (EU) 2023/2854 (EU Data Act). If personal data is involved, Regulation (EU) 2016/679 (GDPR) shall also apply.
5. Version Number: V1.0
6. Effective Date: January 6, 2026

II. Explanation of the Legal Nature of Data

Pursuant to Articles 2 and 3 of the EU Data Act, the data generated by this product during normal use falls into the following categories:

- Product Data: Data automatically generated by connected devices during operation, monitoring, or use;
- Related Service Data: Data generated by digital supporting services provided to realize device functions.

If the relevant data constitutes Personal Data under the General Data Protection Regulation (GDPR) in specific scenarios, its processing shall also comply with the principles of legality, necessity and proportionality,

and security stipulated in the GDPR.

III. Types and Generation of Product Data

(I) Classification by Data Nature

1. Data That May Involve Personal Data

(1) Device user operation records (e.g., login time, device control operations (starting/stopping recording, parameter adjustment));

(2) Basic account information (e.g., user nickname, registration region, used for account identification and security).

2. Non-Personal Data

(1) Device status data: Device operating status (online/offline, battery level (for low-power battery models), remaining storage space, firmware version number, fault diagnosis codes (e.g., addition failure 403)), video storage format (e.g., H.265/MP4), real-time transmission frame rate (e.g., 25fps);

(2) Environmental data: Ambient temperature, light intensity (used for automatic adjustment of night vision mode) collected by the camera, sound decibel value (recorded only when the "sound detection alarm" function is enabled);

(3) Device usage data: Daily recording duration, number of video files, number of remote accesses, Wi-Fi/network information of the device installation location (only Wi-Fi SSID is saved, Wi-Fi password is not stored) (statistical data not associated with user identity).

3. Data Generation Methods

(1) Real-time generation: Continuously generated when the device is in real-time monitoring mode;

(2) Non-real-time generation: Generated only during scheduled recording or alarm triggering;

(3) No video data is generated when the device is in standby or power-off state.

(II) Estimated Data Volume

1. Data Generated by User Interaction

(1) Device operation records adopt two storage methods: DDR temporary storage and SD card/hard disk storage. Among them, the maximum capacity of

DDR storage is 300KB, and the maximum capacity of SD card/hard disk storage is 100MB, adopting a circular overwriting storage mechanism.

(2) Video data: Default alarm recording mode. The size of stored video data varies with the complexity of the environment. The hourly data volume for common storage resolutions is as follows:

- 360P resolution: Approximately 225MB-450MB per hour;
- 1080P resolution: Approximately 450MB-675MB per hour;
- 3MP resolution: Approximately 675MB-900MB per hour;
- 4MP resolution: Approximately 900MB-1.8GB per hour;
- 5MP resolution: Approximately 1GB-1.8GB per hour;
- 4K resolution: Approximately 1.54GB-2.2GB per hour.

2. Data in Standby/Off State

(1) Standby state (device powered on but not recording): The maximum hourly heartbeat data generated by the device is approximately 300KB;

(2) Off state (device powered off): No data is generated.

(III) Data Formats

Data Type	Specific Format
Image Data	JPEG/PNG
Operation Records/Status Data	JSON format (including timestamp, operation type, device status code)
Video Data	Main storage format: H.264/H.265+/MP4; Backup export format: AVI
Environmental Data	TXT format (including temperature, decibel value, and collection time)

(IV) Real-Time Data Generation Capability

1. Supports continuous and real-time data generation: When the device is in "Real-Time Monitoring" mode, video data, environmental data, and device status data are all generated in real-time (delay ≤ 1 second);

2. Non-real-time data scenarios: When the device is in "Scheduled Recording" mode, data is only generated during the set time period (e.g., 18:00 - 24:00), and no real-time data is generated outside the set time period.

(V) Data Storage Locations

1. Local Storage (Default)

(1) Network Camera: Supports Micro SD card storage (maximum 512GB). Video data, operation records, and device status data are preferentially stored in the local SD card;

(2) DVR Kit: Stores data through a built-in hard disk (minimum 500GB SSD, maximum 8TB HDD), centrally storing video data and device management data of all associated cameras.

2. Remote Storage (Optional, Requires Active Activation by User)

Cloud servers are located in data centers within the EU. Users can choose to synchronize video data to the cloud. This location complies with the requirements of the EU General Data Protection Regulation (GDPR), ensuring a high level of privacy protection during data processing and storage;

Relevant video data will only be synchronized to the cloud server after the user actively enables the cloud storage service function and selects the corresponding service plan. If the user does not enable the cloud storage service, the video data will not be synchronized to the remote server. Before activating the service, users need to carefully read the agreement terms to understand the data usage and sharing policies. After activation, users can adjust storage preferences or cancel the service at any time through the in-app settings.

(VI) Data Retention Period

1. Locally Stored Data

(1) Video data adopts a circular overwriting mechanism. When the storage device (e.g., SD card or hard disk) is full, the earliest data is automatically overwritten; users can manually configure the recording mode, including 24/7 recording and alarm recording; users can manually delete or format the storage medium at any time.

(2) Device status data and log records are stored in local storage. When the user formats the SD card or hard disk, this data will be deleted synchronously.

2. Cloud Storage (If Enabled)

(1) Video data (if enabled): According to the cloud storage plan selected by the user (e.g., both free and paid plans retain data for 30 days), the system automatically removes the video content of the earliest day after 30 days, adopting a circular overwriting mechanism;

(2) Pushed image data: Usually stored for 7 days. After 7 days, the image content of the earliest day is automatically deleted, also using a circular overwriting mechanism;

(3) After the user terminates the cloud service or cancels the account, their cloud data will be deleted or anonymized within a reasonable period before being used for any business or analytical purposes.

VII. Explanation of User Rights Related to Data Operations

(I) Data Access Methods

After logging into their personal account through the mobile application supporting the product, users can directly view the following content:

(1) Real-time monitoring screen, providing high-definition real-time video streams to keep you informed of on-site dynamics at any time; historical video data, including local storage and cloud backup, supporting convenient playback by date and time.

(2) Device information: Displays the current status of the device (e.g., online, offline, faulty) and detailed parameters (e.g., resolution, frame rate, storage capacity).

(3) Personal information records: Including user nickname, account details, registration region, etc., used for personalized settings and account security management.

(4) Users have the right to access the data generated by their devices in a direct, convenient, and free manner.

Note: This product currently does not provide end-users with a public Application Programming Interface (API) or Software Development Kit (SDK) for data access. The above situation does not affect users' direct access,

download, or deletion of data generated by their devices in the manner described in this document.

(II) Data Retrieval Methods

1. Mobile App/PC Retrieval

Before first use, users need to agree to the App's User Agreement and Privacy Policy.

(1) Device alarm notification data: Supports retrieval by date and push type (including: humanoid, vehicle-shaped and other alarm types) in the "Messages" function. Retrieval results can be previewed and downloaded;

(2) Video data: Supports retrieval by "time range" (accurate to the minute) and "event type" (including: alarm recording, 24/7 recording) in the "Playback" function. Retrieval results can be previewed and downloaded;

2. Local Storage Retrieval

Connect the DVR/NVR kit to a monitor, control it via the mouse connected to the device, retrieve video data in the local hard disk by "date - time period", and support fast forward and playback operations.

(III) Data Deletion and Control

1. Local Data Erasure

(1) Manually clear App log cache: In the App's "Personal Center - Clear Cache", confirm the deletion of cache data generated by running the App, including app log and device cover cache. The data will be deleted immediately after confirmation;

(2) Restore device to factory settings: Long press the reset button on the device's physical keys for 5 seconds or perform "Restore Factory Settings" on the DVR/NVR kit via the monitor to clear all locally stored information data (including Wi-Fi/network information, recording configuration, device parameter configuration, etc.), but will not delete the video data on the SD card/hard disk.

(3) Delete video data on local SD card/hard disk: Manually format the video data on the SD card/hard disk via the client application or the DVR/NVR kit on the monitor. Once confirmed, the data cannot be recovered;

2. Remote Data Erasure

Cloud storage data: In the video management of the App's "Cloud Storage Playback Interface", select "Delete specified file data" or "Select all

videos". Once confirmed, the data cannot be recovered;

Account cancellation: When a user applies to cancel their personal account, the system will immediately delete all associated remote data (including personal account information, cloud videos, pushed image data, etc.). Once confirmed, the account data cannot be recovered;

VIII. Boundaries Between Trade Secrets and Data Rights

1. Holder of Trade Secrets

Identity: ZOSI

Contact Information: support@zosisecurity.com

2. Trade Secret Identification Method

3. The data access rights disclosed in this document do not involve the disclosure of the following legally protected information: "core algorithms of device firmware" and "generation rules of cloud server data encryption keys". User Notes

The protection of trade secrets does not affect users' legal exercise of their rights to access, use, and delete data generated by their own devices; if users discover a potential leak of trade secrets, they may contact the holder of the trade secrets for handling.

IX. Data-Related Contract Terms

1. Contract Term

If the user activates a cloud service plan, the contract term is consistent with the validity period of the cloud storage plan (e.g., 1 month / 12 months). Whether to renew the contract after expiration depends on the user's actual choice in the app or platform;

There is no fixed contract term for data use. It takes effect from the date the user purchases the product and activates the device, and ends when the device is scrapped or the user abandons the right to use it.

2. Contract Termination Arrangements

Users can terminate the remote cloud service at any time: Click the "Cloud Storage Service" disable button in the App's "Device Settings - Cloud Storage Settings". The contract will terminate when the current plan expires. Unused service duration will not be refunded, and no new cloud data will be generated after termination;

If the user violates the User Agreement or applicable laws, and such behavior directly affects the legality or security of the data service, we have the right to unilaterally terminate the data service and will notify the user via email or SMS 7 days in advance before termination. The user needs to back up necessary data within the notification period;

After the contract is terminated, all remote data will be cleared within a reasonable period, and local data shall be handled by the user themselves.

3. Viewing of Relevant Terms

Details of the User Terms of Service and Privacy Policy can be viewed by users in the "Personal Center - About" section of the App. It fully elaborates on the user's rights, responsibilities, and privacy protection measures when using the service, including relevant terms on data collection, use, and sharing.

X. Compliance Statement

This document strictly complies with the requirements of the EU Data Act (Regulation (EU) 2023/2854, applicable from September 12, 2025), truthfully discloses information related to the collection, transmission, storage of product data and user rights, without any false or omitted content. In accordance with the provisions of the EU Data Act, if subsequent functional upgrades of the product result in changes to data processing rules, this statement will be updated through in-app notifications or other means within a reasonable period before the change, and users will be notified via App push, email, etc. Users can view the updated version in "Messages - System Notifications".