GeoVision GV-Cloud Privacy Compliance

1. Privacy Overview

GeoVision is committed to protecting customer privacy and data security. The GV-Cloud platform incorporates "Privacy by Design" principles from the development phase and adheres to international privacy standards. We ensure that data processing activities are limited to what is necessary to provide, maintain, and optimize security services, providing transparency at every stage of the data lifecycle.

2. Data Collection Scope

GV-Cloud collects the following categories of data to perform its services:

- **Account & Contact Information**: Name, email address, and phone number (for authentication and alert notifications).
- **Device & System Data**: Device IP addresses, firmware versions, system health logs, and connection records.
- **Security Content Data**:
  - **Video Data (VMS)**: Live streams, recorded files, and event snapshots captured by customer cameras.
  - **Access Control Data**: Access logs, user card numbers, IDs, and access event snapshots.
- **Diagnostic & Telemetry Data**: App usage patterns, browser types, and system performance metrics.

3. Data Usage Scope

Collected data is used strictly for the following purposes:

- Providing live monitoring, remote playback, and access control functionalities.
- Delivering user-defined event alerts via email or push notifications.
- Leveraging Edge AI (e.g., human/vehicle detection) to improve event accuracy and minimize unnecessary video transmission.
- Performing system health checks and security updates.

4. Data Ownership Policy

GeoVision treats customers as Data Owners and Controllers, while GeoVision acts as the Data Processor. Customers retain absolute control over their video content, access logs, and user data. GeoVision does not sell raw monitoring content to third parties or use it for advertising.

5. Data Storage Location

To support data localization and reduce latency:

- **Multi-Region Deployment**: Primary data centers are located in the United States (US) and European Union (EU).
- **Automated Routing**: Upon connection, GV-Cloud automatically detects the device's IP location and routes data to the nearest appropriate regional data center.

6. Data Retention Policy

Retention periods are determined by the customer's selected license plan:

- **Video & Snapshots (VMS)**: Supports cyclic storage for 3, 7, 15, or 30 days.
- **Access Logs (Access Control)**: Supports retention for 90, 180, or 365 days.
- **Account Information**: Retained for the duration of the active account until termination or deletion request.

7. Data Deletion Policy

- **Automated Deletion**: Video and event data are automatically overwritten or permanently deleted from cloud servers once the retention period expires.
- **Manual Deletion**: Administrators can manually delete specific devices, user information, or historical logs via the management interface.
- **Termination Deletion**: Upon service termination and account closure, all customer-related data is purged from the system.

8. Data Access Control

- **Role-Based Access Control (RBAC)**: Supports Master User, Region Manager, and Normal User roles to precisely limit access to specific regions and cameras.
- **Multi-Factor Authentication (MFA/2FA)**: Enforces secondary login verification via SMS or Email to prevent unauthorized access even if passwords are compromised.
- **Internal Access Restrictions**: By default, GeoVision personnel cannot view live video or private logs without explicit customer authorization.

9. Customer Data Protection

- **Transmission Encryption**: Uses TLS 1.2 / TLS 1.3, HTTPS, and Secure WebSocket (WSS) to protect all data transmitted between devices and the cloud.
- **At-Rest Encryption:** Video clip files and credentials stored on cloud servers are protected by AES-256 encryption.

10. Compliance Status

- **General Data Protection Regulation (GDPR):** Compliant. Provides rights for data access, rectification, erasure, and portability.
- **Payment Card Industry Data Security Standard (PCI DSS):** Subscription payment processes are handled by PCI-compliant third-party gateways.

11. Privacy Risk Control

- **Privacy Masking**: Supports configurable masking zones at the camera level to obscure sensitive areas (e.g., private windows), ensuring they are not recorded or uploaded.
- **Audit Logging**: The system records user activities, ensuring operational transparency.

12. Customer Rights & Responsibilities

- **Customer Rights**: Customers have the right to access, download, modify, or delete their personal data and configurations stored in the cloud.
- **Customer Responsibilities**: Customers are responsible for managing account credentials, enforcing strong passwords, assigning appropriate permissions, and ensuring surveillance activities comply with local laws.