

Date: [Insert Date]

To: [Recipient Name/Data Center Management]

Location: [Data Center Site/City, Country]

Subject: ADVISORY: Overseas Biometric Security Compliance Requirements

Dear [Name/Management Team],

This letter serves as a formal advisory regarding the biometric security protocols and data privacy compliance requirements for our overseas data center facilities located in [Country].

To ensure continued alignment with international data protection regulations (such as GDPR, CCPA, or local equivalents), all biometric access control systems—including fingerprint, iris, and facial recognition—must adhere to the following standards:

- **Data Minimization:** Only essential biometric templates should be collected. Raw biometric images must not be stored on local servers.
- **Encryption:** All biometric data must be encrypted at rest and in transit using [Insert Standard, e.g., AES-256] encryption.
- **Consent and Disclosure:** Explicit written consent must be obtained from all personnel before biometric enrollment. Privacy notices must be clearly displayed at entry points.
- **Audit Logs:** Access logs must be maintained for a period of [Number] months and made available for compliance audits upon request.
- **Cross-Border Transfer:** Biometric data must not be transferred outside of the host country without verifying legal data transfer agreements (SCCs).

Please review your current physical security operations and submit a Compliance Confirmation Report by [Date]. Failure to meet these standards may result in a formal security audit or service level agreement (SLA) review.

For technical guidance or clarification on local regulatory requirements, please contact the Global Security Compliance Office.

Sincerely,

[Your Name]

[Your Title]

[Company Name]

[Contact Information]