AMS SaaS (Access Manager Suite – Software as a Service) DATA PROTECTION STATEMENT

Version: 1.2
Last Updated: January 2026

Overview

This Data Protection Statement outlines the security measures and data handling practices implemented in the AMS SaaS (Access Manager Suite – Software as a Service) cloud platform and associated ACTAtek™ devices to ensure the highest level of protection for user data, particularly biometric information.

1. Biometric Data Protection

1.1 Data Storage Format

1.1.1 Fingerprint Biometric Data

- **Template-Based Storage**: Fingerprint biometric data is NOT stored as images or photographs. Instead, the system converts biometric information into encrypted fingerprint templates.
- **Non-Reversible Process**: These templates are mathematical representations that cannot be reverse-engineered to recreate the original biometric image.
- **Enhanced Privacy**: This approach ensures that raw fingerprint biometric data is never stored, transmitted, or exposed in any form.

1.1.2 Facial Recognition Data

- **Photo Capture and Storage**: For ACTAtek devices equipped with facial recognition capabilities and built-in CMOS cameras, the system stores photographs.
- **Dual Storage Locations**: Captured photographs are stored both:
  - Locally on the ACTAtek device itself
  - In the AMS SaaS cloud database for centralized management
- **User Consent Requirement**: **IMPORTANT - The capture and storage of photographs requires explicit user consent.** Organizations must obtain proper consent from individuals before the enrollment.
- **Template Processing**: In addition to photo storage, facial biometric data is also processed into encrypted templates for faster matching operations.

1.2 Encryption Standards

The AMS SaaS platform employs industry-leading encryption for biometric data:

- **AES-256 Bit Encryption**: All biometric templates are encrypted using Advanced Encryption Standard with 256-bit keys, providing military-grade security.
- **Key Management**: Encryption keys are securely managed and regularly rotated to maintain data integrity.

1.3 Compliance Standards

Jakin® biometric templates are compliant with internationally recognized standards:

- **ISO 19794-2**: International standard for biometric data interchange formats
- **ANSI/INCITS 378**: American National Standard for fingerprint minutiae data
- **ILO SID**: International Labour Organization Seafarers' Identity Documents standards

These certifications ensure interoperability, security, and compliance with global data protection requirements.

2. Data Transmission Security

2.1 TLS 1.3 Encryption

- **State-of-the-Art Protocol**: All communication between ACTAtek™ devices and AMS SaaS cloud servers is encrypted using Transport Layer Security (TLS) version 1.3.
- **End-to-End Protection**: TLS 1.3 provides enhanced security with improved encryption algorithms and faster handshake protocols.

2.2 Network Infrastructure Compatibility

- **VPN Support**: Data transmissions remain secure even when devices operate through Virtual Private Networks (VPNs).
- **Firewall Compatibility**: The system is designed to function seamlessly behind corporate firewalls without compromising security.
- **Port Security**: Uses standard secure ports with configurable options for enterprise network requirements.

3. Data Integrity and Availability

3.1 Local Storage Capability

- **Offline Operation**: ACTAtek™ devices store data locally, allowing continuous operation even during network interruptions.

- **Data Buffering**: Events, logs, and transactions are buffered on the device when cloud connectivity is unavailable.

3.2 Automatic Synchronization

- **Seamless Reconnection**: When network connectivity is restored, devices automatically sync all buffered data to the cloud platform.
- **Zero Data Loss**: The system ensures no data is lost during connection interruptions, maintaining complete audit trails and records.
- **Conflict Resolution**: Intelligent synchronization algorithms handle any potential conflicts during data reconciliation.

4. User Consent and Privacy Rights

4.1 Consent Requirements for Photo Capture

4.1.1 Mandatory Consent for Facial Recognition Organizations using ACTAtek Facial models or devices with built-in CMOS cameras MUST obtain explicit, informed consent from individuals before:

- Capturing photographs for facial recognition purposes
- Storing photographs on ACTAtek devices
- Uploading and storing photographs to the AMS SaaS platform
- Processing facial biometric data for identification

4.1.2 Consent Best Practices Organizations should implement the following consent practices:

- **Clear Communication**: Inform individuals about:
  - What data is being collected (photographs and facial biometric templates)
  - Where the data will be stored (device and cloud)
  - How the data will be used (identification and access control)
  - How long the data will be retained
  - Their rights regarding their biometric data
- **Voluntary Participation**: Ensure participation in facial recognition systems is voluntary where legally required
- **Consent Documentation**: Maintain records of all consent agreements for compliance purposes

4.1.3 Consent Statement Template Organizations should use a consent statement similar to the following:

"I consent to the capture and storage of my photograph and facial biometric data by [Organization Name] for the purpose of identity verification and access control. I understand that my photograph will be stored on ACTAtek devices and in the AMS SaaS cloud platform, and will be used solely for authorized access control purposes. I understand I may withdraw this consent by contacting [Organization Contact Information]."

4.2 Individual Rights

4.2.1 Right to Access Individuals have the right to request access to their stored photographs and biometric data.

4.2.2 Right to Deletion Individuals may request deletion of their photographs and biometric data. Organizations must have procedures in place to honor such requests in accordance with applicable laws.

4.2.3 Right to Withdraw Consent Individuals may withdraw their consent at any time. Upon withdrawal, organizations should promptly delete the individual's photographs and biometric data unless retention is required by law.

4.2.4 Data Portability Where applicable, individuals may request a copy of their biometric data in a portable format.

4.3 Organizational Responsibilities

4.3.1 Consent Management Client organizations are responsible for:

- Obtaining and documenting proper consent before enrollment
- Maintaining consent records
- Providing individuals with information about their rights
- Responding to data subject requests (access, deletion, etc.)
- Ensuring compliance with applicable biometric privacy laws

4.3.2 Legal Compliance Organizations must comply with all applicable biometric privacy laws and regulations, including but not limited to:

- Biometric Information Privacy Act (BIPA) in applicable jurisdictions
- General Data Protection Regulation (GDPR) in the European Union
- California Consumer Privacy Act (CCPA) in California
- Other local, state, and national biometric privacy laws

4.3.3 Employee/User Notification Organizations should provide clear notice to employees or users about:

- The biometric system being used
- The purpose of biometric collection
- The retention period for biometric data
- How to exercise their privacy rights

5. Access Control and Authentication

5.1 User Access Management

- **Role-Based Access Control (RBAC)**: Administrators can define granular permissions based on user roles and responsibilities.
- **Audit Logging**: All access and modifications are logged for security auditing and compliance purposes.

5.2 Device Authentication

- **Secure Device Registration**: Each ACTAtek™ device must be properly authenticated with the compatible firmware versions before syncing with AMS SaaS.

---

6. Data Residency and Retention

6.1 Data Location

- Client data is stored in secured cloud infrastructure.
- Data residency options may be available based on regulatory requirements.

6.2 Data Retention

- Data is retained according to client specifications and applicable legal requirements.
- Secure deletion procedures are implemented when data retention periods expire or upon client request.

---

7. Compliance and Certifications

Jakin® is committed to maintaining compliance with applicable data protection regulations, including:

- General Data Protection Regulation (GDPR) where applicable
- **Biometric Privacy Laws**: Organizations using facial recognition features must comply with applicable biometric privacy laws such as:
    - Biometric Information Privacy Act (BIPA) and similar state laws
    - California Consumer Privacy Act (CCPA) regarding biometric data
    - Other applicable local, state, national, and international biometric privacy regulations
- Industry-specific security standards and best practices
- Regular security audits and vulnerability assessments

Client Responsibility: Clients are solely responsible for ensuring compliance with all biometric privacy laws applicable to their jurisdiction and operations, including obtaining necessary consents and providing required notices.

8. Incident Response

8.1 Security Monitoring

- Continuous monitoring of systems for potential security threats
- Automated alerts for suspicious activities or unauthorized access attempts

8.2 Incident Management

- Timely notification to affected parties in accordance with applicable regulations

9. Client Responsibilities

To maintain the security of the AMS SaaS environment, clients are responsible for:

- Maintaining secure credentials and access controls
- Promptly reporting any suspected security incidents
- Ensuring proper physical security of ACTAtek™ devices
- Keeping device firmware and software updated as recommended
- **Compliance with Privacy Laws**: Ensuring compliance with all applicable biometric privacy laws and regulations in their jurisdiction

10. Updates and Modifications

Jakin® reserves the right to update security measures and data protection practices as technology evolves and new threats emerge. Clients will be notified of significant changes to data protection practices.

11. Contact Information

For questions regarding data protection or to report security concerns:

Email: support@actatek.com
Website: www.jakinid.com/support

This Data Protection Statement is subject to the terms and conditions outlined in the AMS SaaS Terms and Conditions Statement and End User License Agreement.