Data Protection Statement for EntropyX

Effective Date: July 9, 2025
Last Updated: July 9, 2025
Document Version: 1.0

Executive Summary

EntropyX is designed as a privacy-first, enterprise-grade compression solution that operates under a **zero external data collection** architecture. This Data Protection Statement outlines the technical measures, security controls, and compliance frameworks implemented to protect organizational data during file processing operations.

Key Commitment: Under current ownership, EntropyX processes all data locally on user devices with no external data transmission, storage, or analysis.

1. Data Processing Architecture

1.1 Local Processing Model

Current Implementation:

- **100% Local Processing** - All file compression, decompression, and conversion occurs entirely on user devices
- **No Cloud Dependencies** - No external servers, APIs, or cloud services involved in data processing
- **Zero Data Transmission** - File contents never leave the user's local environment
- **Isolated Operations** - Each file processing operation is independent and self-contained

1.2 Data Flow Architecture

The software implements a strictly local data flow where user files are validated locally, processed in system memory, and output to local storage without any external network communication or data transmission.

1.3 Memory Management

- **In-Memory Processing** - Files processed in system RAM without persistent intermediate storage
- **Automatic Cleanup** - Memory is cleared after processing operations complete

- **No Persistent Caching** - No temporary file storage beyond active processing sessions
- **Secure Memory Handling** - Sensitive data is not retained in memory after operations

2. Data Categories and Handling

2.1 Data NOT Collected or Processed Externally

Under current ownership, EntropyX does NOT collect, store, or transmit:

File Content Data:

- Document contents, text, or media data
- File metadata beyond local processing requirements
- Compression statistics or processing metrics to external systems
- File checksums or integrity hashes to external systems

User Information:

- Personal identifiers or contact information
- User behavior patterns or usage analytics to external systems
- System configuration details to external systems
- Network information or IP addresses to external systems

Organizational Data:

- Corporate file structures or naming conventions to external systems
- Business processes or workflow patterns
- Organizational policies or procedures
- Internal system configurations

2.2 Local Audit Data (Device-Only Storage)

The software generates comprehensive audit logs that are stored exclusively on local devices and never transmitted externally.

Local Audit Components:

- **Session Tracking** - Unique session identifiers for audit trail continuity

- **File Operations** - Processing timestamps, file sizes, compression ratios, and algorithm selection
- **Security Events** - File validation results, access control verification, and security violations
- **Performance Metrics** - Processing duration, resource utilization, and optimization data
- **Error Information** - Exception details and diagnostic information for troubleshooting
- **User Activity** - Application usage patterns and feature utilization within local environment

Audit Storage Characteristics:

- **Primary Location** - System-level logs directory with appropriate permissions
- **Fallback Storage** - Application directory if system location unavailable
- **Automatic Rotation** - Prevents excessive storage usage through size and time-based rotation
- **Integrity Protection** - Cryptographic hashes prevent unauthorized log modification

2.3 Log Data Security Features

- **Local Storage Only** - All audit data remains on user devices
- **Integrity Verification** - SHA-256 hashing protects against log tampering
- **Access Control** - Logs accessible only through local file system permissions
- **Rotation Management** - Automated log rotation prevents storage exhaustion

3. Security Controls and Technical Implementation

3.1 Input Validation and File Security

Comprehensive File Validation:

- **Path Traversal Protection** - Prevents unauthorized directory access through path normalization
- **File Type Validation** - Restricts processing to approved file extensions and MIME types

- **Size Limitations** - Enforces maximum file size limits (500MB default) to prevent resource exhaustion
- **Content Integrity** - Validates file structure and format before processing
- **Access Verification** - Confirms user has appropriate file system permissions

Filename Security:

- **Character Sanitization** - Removes dangerous characters that could enable injection attacks
- **Reserved Name Protection** - Prevents processing of system-reserved filenames
- **Length Limitation** - Enforces maximum filename length to prevent buffer overflow conditions
- **Control Character Filtering** - Removes non-printable characters that could cause system issues

3.2 Encryption Implementation

Multi-Layer Encryption Architecture:

- **Primary Encryption** - AES-256 encryption using Fernet symmetric encryption when cryptographic libraries are available
- **Key Management** - Secure local key generation and storage using system-provided security APIs
- **Fallback Encryption** - Custom encryption implementation ensuring data protection when standard libraries unavailable
- **Key Storage Security** - Encryption keys stored locally with hidden file attributes on Windows systems

Encryption Characteristics:

- **Algorithm Strength** - Industry-standard AES-256 encryption for maximum security
- **Authentication** - Cryptographic authentication prevents tampering with encrypted data
- **Local Key Control** - All encryption keys generated and stored locally under user control

- **Integrity Verification** - Encrypted data includes integrity verification to detect corruption

3.3 Security Event Monitoring

Comprehensive Security Logging:

- **Event Classification** - Multiple levels of security events from informational to critical
- **Real-time Detection** - Immediate logging of security-relevant events during processing
- **Detailed Context** - Security events include timestamp, user context, and detailed event information
- **Tamper Detection** - Integrity verification prevents unauthorized modification of security logs

Security Events Monitored:

- **File Access Violations** - Attempts to access unauthorized files or directories
- **Validation Failures** - Files that fail security or integrity validation
- **Size and Type Violations** - Files exceeding size limits or using prohibited file types
- **Encryption Events** - Key generation, encryption operations, and decryption activities
- **System Integrity** - Application integrity verification and dependency validation

3.4 Application Security Features

Built-in Security Measures:

- **Application Integrity Verification** - Internal validation of application components and dependencies
- **Dependency Verification** - Validation of required third-party components (FFmpeg, Ghostscript)
- **Error Handling** - Secure error messages that don't expose sensitive system information
- **Resource Management** - Protection against resource exhaustion and denial of service conditions

4. Third-Party Components and Dependencies

4.1 External Software Dependencies

Required Third-Party Components:

- **FFmpeg** - Media processing engine for audio and video compression (LGPL/GPL licensed)
- **Ghostscript** - PDF processing and optimization engine (AGPL licensed)
- **Microsoft Word** - Document conversion engine for DOCX to PDF conversion (Windows only)
- **Python Libraries** - Standard libraries for compression, encryption, and system operations

4.2 Third-Party Security Model

Local Processing Guarantee:

- **No Network Communication** - All third-party components configured for offline, local operation
- **Subprocess Isolation** - External components run in isolated process spaces
- **Input Validation** - All data passed to third-party components is validated and sanitized
- **Output Verification** - Results from third-party components are validated before use

Component Security:

- **Version Control** - Specific, tested versions of third-party components are used
- **Execution Safety** - Components executed with validated parameters and timeout protection
- **Error Containment** - Failures in third-party components don't compromise system security
- **Local Resource Only** - Components operate exclusively on local system resources

4.3 Dependency Management

Security Verification:

- **Component Detection** - Automatic detection and verification of required dependencies
- **Version Validation** - Confirmation that installed components meet security requirements
- **Isolation Enforcement** - Third-party components operate in controlled execution environments
- **Failure Handling** - Graceful degradation when optional components are unavailable

5. Compliance Framework Alignment

5.1 Privacy Regulation Compliance

General Data Protection Regulation (GDPR):

- **Data Minimization** - No personal data collection beyond operational necessity
- **Purpose Limitation** - Data processing limited exclusively to compression functionality
- **Storage Limitation** - No long-term data retention beyond local audit logs
- **Transparency** - Complete documentation of all data processing activities
- **User Control** - Local processing ensures complete user control over personal data

California Consumer Privacy Act (CCPA):

- **No Personal Information Sale** - Zero data collection eliminates data selling concerns
- **Transparency Requirements** - Full disclosure of data handling practices
- **Consumer Rights** - Complete user control over local data processing
- **Opt-Out Compliance** - Users can disable audit logging through application settings

Children's Online Privacy Protection Act (COPPA):

- **Age Restriction** - Software explicitly not intended for users under 13 years
- **No Data Collection** - Zero external data collection policy protects users of all ages
- **Parental Oversight** - Local processing enables complete parental control and oversight

5.2 Security Framework Compliance

NIST Cybersecurity Framework:

- **Identify** - Comprehensive file validation and risk assessment capabilities
- **Protect** - Encryption, access controls, and input validation measures
- **Detect** - Extensive audit logging and security event monitoring
- **Respond** - Structured error handling and security incident logging
- **Recover** - File integrity verification and data validation procedures

ISO 27001 Information Security Management:

- **Information Security Controls** - Documented security measures and procedures
- **Risk Management** - File validation and security assessment processes
- **Access Control** - User authentication and file permission verification
- **Cryptographic Controls** - Industry-standard encryption implementation
- **Audit Trail Management** - Comprehensive logging and monitoring capabilities

SOC 2 Security Controls:

- **Security** - Encryption, access controls, and secure processing procedures
- **Availability** - Reliable file processing with comprehensive error handling
- **Processing Integrity** - File integrity verification and validation procedures
- **Confidentiality** - Local processing with no external data exposure

5.3 Technical Security Standards

NIST Privacy Framework:

- **Privacy Risk Management** - Comprehensive risk assessment and mitigation
- **Data Processing Governance** - Clear policies for data handling and processing
- **Individual Participation** - Complete user control over data processing activities

CIS Critical Security Controls:

- **Asset Inventory** - System information gathering and component verification
- **Secure Configuration** - Hardened default settings and security configurations

- **Access Control** - File permission validation and user authorization
- **Audit Log Management** - Comprehensive audit trail generation and protection

OWASP Security Guidelines:

- **Input Validation** - Comprehensive file and parameter validation procedures
- **Error Handling** - Secure error messages that don't expose sensitive information
- **Data Protection** - Encryption and secure data handling procedures
- **Logging and Monitoring** - Security event detection and audit trail generation

6. Data Retention and Lifecycle Management

6.1 Data Processing Lifecycle

Processing Workflow:

1. **Input Validation** - Security and integrity verification of input files
2. **Local Processing** - Compression, decompression, or conversion operations
3. **Output Generation** - Creation of processed files in local storage
4. **Memory Cleanup** - Immediate clearing of sensitive data from system memory
5. **Audit Recording** - Local logging of operation metadata and results

6.2 Data Retention Policies

Current Retention Model:

- **No Persistent File Storage** - File contents never stored beyond active processing
- **Local Audit Retention** - Configurable retention periods for audit logs (default: 30 days)
- **Automatic Log Management** - Rotation prevents excessive storage usage
- **Secure Deletion** - Immediate cleanup of temporary data and processing artifacts

6.3 End-of-Life Data Handling

Software Removal Procedures:

- **Complete Uninstallation** - All software components and data files removed
- **Secure Key Deletion** - Encryption keys securely destroyed during uninstallation

- **Audit Log Options** - Optional preservation of audit logs for compliance requirements
- **Verification Procedures** - Confirmation of complete data and component removal

7. Enterprise Security Considerations

7.1 Organizational Deployment

Enterprise-Ready Features:

- **Multi-Device Support** - Software can be deployed across unlimited organizational devices
- **Local Administrative Control** - Complete organizational control over software configuration
- **Audit Trail Generation** - Comprehensive logging supports organizational compliance requirements
- **Security Integration** - Compatible with existing organizational security policies

7.2 Compliance Support

Regulatory Framework Support:

- **Audit Trail Generation** - Detailed logs support SOX, FISMA, and other audit requirements
- **Data Protection** - Local processing model supports HIPAA, FERPA, and privacy regulations
- **Security Controls** - Technical measures align with industry security frameworks
- **Documentation** - Complete documentation supports compliance verification activities

7.3 Risk Management

Security Risk Mitigation:

- **Attack Surface Minimization** - No network communication reduces attack vectors
- **Data Exposure Prevention** - Local processing eliminates data breach risks from external systems
- **Component Isolation** - Third-party dependencies operate in controlled environments

- **Comprehensive Monitoring** - Security event logging enables rapid incident detection

8. Future Considerations and Ownership Transfer

8.1 Ownership Transfer Commitments

User Protection Guarantees:

- **30-Day Advanced Notice** - Minimum notification period for any ownership changes
- **Complete Transparency** - Full disclosure of new data handling practices
- **User Choice** - Right to discontinue use before new practices take effect
- **Transition Support** - Technical assistance during ownership transition period

8.2 Potential Future Changes

Possible Data Collection Evolution:

- **Usage Analytics** - Aggregated, anonymized usage statistics collection
- **Performance Metrics** - System performance and optimization data gathering
- **Error Reporting** - Automated crash and error reporting capabilities
- **Feature Telemetry** - Analysis of feature adoption and usage patterns

Continued Commitments:

- **File Content Protection** - Commitment to never access or transmit file contents
- **Local Processing Priority** - Maintain local processing as the primary operational model
- **User Control** - Preserve user control over data handling and privacy settings
- **Compliance Continuity** - Continue support for enterprise compliance frameworks

8.3 Data Protection Continuity

Transition Protections:

- **Existing Data Safeguards** - Current protections maintained during ownership transition
- **Clear Communication** - Transparent disclosure of any changes to data handling practices

- **Termination Rights** - Ability to discontinue use without penalty during transition
- **Migration Support** - Technical assistance for transitioning to alternative solutions

9. Contact Information and Support

9.1 Data Protection Inquiries

Primary Contact: entropyxcompression@gmail.com

Response Commitment: Data protection inquiries receive responses within 72 hours during business days.

Supported Inquiry Types:

- Data protection questions and technical concerns
- Security incident reporting and vulnerability disclosure
- Compliance verification and audit support requests
- Technical implementation and security architecture questions

9.2 Data Protection Responsibility

Data protection inquiries are handled by qualified technical personnel with expertise in:

- Security architecture and implementation details
- Regulatory compliance and legal requirements
- Customer support and technical assistance
- Privacy policy interpretation and application

10. Document Maintenance and Continuous Improvement

10.1 Document Management

- **Version Control** - Systematic versioning and change tracking
- **Regular Review** - Annual review cycle or upon significant changes
- **Change Notification** - User notification of material changes through software updates
- **Archive Maintenance** - Historical versions available upon request

10.2 Ongoing Enhancement

Continuous Security Improvement:

- **Security Assessment** - Regular evaluation of security architecture and controls
- **Compliance Monitoring** - Ongoing alignment with evolving regulatory frameworks
- **User Feedback Integration** - Incorporation of user requirements and feedback
- **Industry Standards Adaptation** - Updates to reflect evolving security and privacy standards

---

This Data Protection Statement demonstrates EntropyX's commitment to enterprise-grade data protection through comprehensive technical implementation, regulatory compliance alignment, and transparent documentation of data handling practices.

Document Classification: Public
Last Updated: July 9, 2025