

DATA RETENTION POLICY

Company: Convo, Inc.

Effective Date: September 1st, 2025

Version: 1.0

Owner: Data Protection Officer (markus@itsconvo.com)

Review Frequency: Annually

1. PURPOSE AND SCOPE

1.1 Purpose

This policy establishes clear guidelines for the retention, deletion, and lifecycle management of all data collected and processed by Convo to ensure compliance with legal requirements, regulatory obligations, and customer commitments.

1.2 Scope

This policy applies to:

- All Personal Data processed by Convo
- Customer conversation data (audio, transcripts, metadata)
- User account and profile information
- System logs and technical data
- Business records and communications
- Backup and archived data

1.3 Legal Framework

This policy ensures compliance with:

- EU General Data Protection Regulation (GDPR)
 - California Consumer Privacy Act (CCPA)
 - Spanish Data Protection Act (LOPDGDD)
 - Industry-specific regulations
 - Customer contractual obligations
-

2. DATA CATEGORIES AND RETENTION PERIODS

2.1 Conversation Data

Audio Recordings

- **Default Retention:** 30 days from recording date
- **Customer Configurable:** 1 day to 7 years
- **Automatic Deletion:** Yes, unless extended by customer

- **Legal Basis:** Customer contract and legitimate interests

Conversation Transcripts

- **Default Retention:** 30 days from creation date
- **Customer Configurable:** 1 day to 7 years (must match audio retention)
- **Automatic Deletion:** Yes, synchronized with audio deletion
- **Legal Basis:** Customer contract and legitimate interests

Conversation Metadata

- **Default Retention:** 30 days from recording date
- **Customer Configurable:** 1 day to 7 years
- **Includes:** Timestamps, duration, participant identifiers, call quality metrics
- **Automatic Deletion:** Yes, synchronized with conversation data
- **Legal Basis:** Customer contract and legitimate interests

2.2 Customer Account Data

User Profile Information

- **Retention Period:** Duration of customer relationship + 90 days
- **Includes:** Names, email addresses, job titles, phone numbers
- **Deletion Trigger:** Account termination or customer request
- **Legal Basis:** Customer contract and legitimate interests

Authentication Data

- **Retention Period:** Duration of customer relationship + 30 days
- **Includes:** Login credentials (hashed), MFA settings, session tokens
- **Deletion Trigger:** Account termination
- **Legal Basis:** Security and legitimate interests

Billing and Payment Information

- **Retention Period:** 7 years from last transaction (tax/legal requirements)
- **Includes:** Invoices, payment records, tax information
- **Deletion Trigger:** Legal retention period expiry
- **Legal Basis:** Legal obligation and legitimate interests

2.3 System and Security Data

Access Logs

- **Retention Period:** 1 year from creation
- **Includes:** Login attempts, data access, system interactions
- **Deletion Trigger:** Automatic after 1 year

- **Legal Basis:** Security monitoring and legitimate interests

Security Incident Logs

- **Retention Period:** 7 years from incident resolution
- **Includes:** Incident reports, forensic data, remediation actions
- **Deletion Trigger:** Legal requirements satisfied
- **Legal Basis:** Legal obligation and legitimate interests

System Performance Logs

- **Retention Period:** 90 days from creation
- **Includes:** System metrics, error logs, performance data
- **Deletion Trigger:** Automatic after 90 days
- **Legal Basis:** Legitimate interests

2.4 Business Communications

Customer Support Records

- **Retention Period:** 3 years from last interaction
- **Includes:** Support tickets, email communications, chat logs
- **Deletion Trigger:** Automatic after 3 years
- **Legal Basis:** Customer service and legitimate interests

Marketing Communications

- **Retention Period:** 3 years from last engagement or unsubscribe
- **Includes:** Email campaigns, consent records, preference data
- **Deletion Trigger:** Unsubscribe + 90 days or 3 years inactive
- **Legal Basis:** Consent or legitimate interests

3. RETENTION SCHEDULE MATRIX

Data Category	Default Period	Customer Configurable	Auto-Delete	Legal Minimum
Audio Record-ings	30 days	1 day - 7 years	Yes	None
Transcripts	30 days	1 day - 7 years	Yes	None
Metadata	30 days	1 day - 7 years	Yes	None
User Profiles	Relationship + 90 days	No	Yes	None
Authentication	Relationship + 30 days	No	Yes	None

Data Category	Default Period	Customer Configurable	Auto-Delete	Legal Minimum
Billing Records	7 years	No	Yes	7 years
Access Logs	1 year	No	Yes	None
Incident Logs	7 years	No	No	7 years
Support Records	3 years	No	Yes	None
Marketing Data	3 years	No	Yes	None

4. DATA DELETION PROCEDURES

4.1 Automated Deletion

Daily Automated Process:

- Scans all data categories for expired retention periods
- Generates deletion queue with verification checksums
- Executes secure deletion following technical standards
- Logs all deletion activities with timestamps and data volumes
- Generates daily deletion reports for review

Technical Implementation:

- **Database Records:** Cryptographic deletion of encryption keys + data overwriting
- **File Systems:** Multi-pass secure deletion (DoD 5220.22-M standard)
- **Backup Systems:** Deletion from all backup copies within 30 days
- **Cloud Storage:** Immediate deletion from primary storage, backup deletion per schedule

4.2 Manual Deletion (Customer Requests)

Process Timeline:

1. **Request Received:** Customer deletion request via email or dashboard
2. **Verification:** Confirm customer identity and scope of request (24 hours)
3. **Impact Assessment:** Determine affected systems and data (48 hours)
4. **Deletion Execution:** Secure deletion from all systems (within 30 days)
5. **Verification:** Confirm complete deletion and provide certificate

Customer Request Methods:

- **Dashboard:** Self-service deletion for specific conversations

- **Email Request:** ivan@itsconvo.com for bulk or account deletion
- **API:** Programmatic deletion for enterprise customers
- **Support Ticket:** Guided deletion with customer support

4.3 Account Termination Process

Upon Customer Account Termination:

1. **Immediate:** Disable access to all customer data
2. **Within 7 days:** Export customer data if requested
3. **Within 90 days:** Complete deletion of all customer data
4. **Verification:** Provide certificate of deletion upon request

Grace Period Data Recovery:

- **30-day grace period** for accidental account termination
 - Customer data preserved but inaccessible during grace period
 - After 30 days, standard deletion timeline applies
-

5. DATA SUBJECT RIGHTS

5.1 Right to Erasure (Right to be Forgotten)

Scope: Data subjects can request deletion of their Personal Data

Timeline: Within 30 days of verified request

Process:

1. Verify data subject identity
2. Assess legal grounds for retention
3. Execute deletion across all systems
4. Notify any data recipients
5. Provide confirmation to data subject

Exceptions to Deletion:

- Legal obligations requiring retention
- Legitimate interests overriding data subject rights
- Active legal proceedings or regulatory investigations

5.2 Data Portability

Scope: Data subjects can request their data in machine-readable format

Timeline: Within 30 days of verified request

Format: JSON format with structured data export

Delivery: Secure download link or encrypted email

5.3 Rectification and Restriction

Rectification: Data corrections within 5 business days

Restriction: Data processing limitation within 24 hours when requested

6. BACKUP AND ARCHIVAL RETENTION

6.1 Backup Strategy

Backup Schedule:

- **Real-time:** Continuous replication to secondary systems
- **Daily:** Full system backups retained for 30 days
- **Weekly:** Weekly backups retained for 12 weeks
- **Monthly:** Monthly backups retained for 12 months
- **Annual:** Yearly backups retained for legal requirements

6.2 Backup Deletion Synchronization

- Customer data deletion requests propagate to all backup systems
- Maximum 30-day window for backup deletion completion
- Automated verification of deletion across all backup sets
- Exception handling for off-site or archival backups

6.3 Long-term Archival

Legal Requirement Archives:

- Financial records: 7 years (tax law requirements)
- Security incidents: 7 years (regulatory requirements)
- Contract records: Duration + 6 years (statute of limitations)

Archive Security:

- Encrypted storage with separate key management
 - Access logging and approval workflows
 - Regular integrity verification
 - Geographic distribution for disaster recovery
-

7. CUSTOMER CONFIGURATION OPTIONS

7.1 Retention Period Settings

Available Options:

- **Minimum:** 1 day (for testing/development)
- **Default:** 30 days (standard business use)

- **Extended:** Up to 7 years (compliance/legal requirements)
- **Custom:** Specific periods for different data types

Configuration Methods:

- **Dashboard Settings:** Self-service configuration by customer admins
- **API Configuration:** Programmatic control for enterprise customers
- **Bulk Configuration:** Customer support assistance for large-scale changes

7.2 Deletion Preferences

Customer Options:

- **Automatic:** Standard deletion per retention schedule
- **Manual:** Customer-initiated deletion only
- **Hybrid:** Automatic with manual override capabilities
- **Immediate:** Deletion upon conversation end (special use cases)

7.3 Legal Hold Functionality

Enterprise Features:

- Suspend deletion for legal proceedings
- Granular hold controls (by date range, user, or data type)
- Audit trail of hold actions
- Automatic hold release with legal approval

8. COMPLIANCE MONITORING

8.1 Retention Compliance Dashboard

Real-time Monitoring:

- Data volumes by retention category
- Upcoming deletion schedules
- Failed deletion attempts
- Customer configuration changes
- Legal hold status

8.2 Audit Trail Requirements

Comprehensive Logging:

- All data creation events with timestamps
- Retention period assignments and changes
- Deletion activities (automatic and manual)
- Customer requests and responses
- System exceptions and error handling

Log Retention: 7 years for all retention-related activities

8.3 Regular Compliance Reviews

Monthly Reviews:

- Deletion activity reports
- Failed deletion analysis
- Customer request response times
- Compliance exception reports

Quarterly Reviews:

- Policy effectiveness assessment
 - Legal requirement updates
 - Customer feedback integration
 - Process improvement identification
-

9. EXCEPTION HANDLING

9.1 Legal Hold Exceptions

When legal hold is required:

- Immediate suspension of deletion activities for affected data
- Documentation of legal basis and scope
- Regular review of hold necessity
- Secure isolation of held data

9.2 Technical Failure Exceptions

When automated deletion fails:

- Immediate alert to technical team
- Manual deletion within 48 hours
- Root cause analysis and system remediation
- Customer notification if deadlines at risk

9.3 Regulatory Investigation Exceptions

During regulatory investigations:

- Preserve relevant data beyond normal retention
 - Maintain detailed access and modification logs
 - Coordinate with legal counsel on retention requirements
 - Resume normal deletion after investigation conclusion
-

10. DATA TRANSFER AND MIGRATION

10.1 System Migrations

During system upgrades or migrations:

- Retention periods transfer with data
- No extension of retention periods due to migration
- Verification of successful data transfer
- Secure deletion of old system data

10.2 Vendor Changes

When changing service providers:

- Ensure data deletion from previous vendor
 - Transfer retention schedules to new vendor
 - Maintain audit trail across transition
 - Customer notification of any retention impacts
-

11. TRAINING AND AWARENESS

11.1 Staff Training

All Employees:

- Annual data retention awareness training
- Understanding of data lifecycle and deletion requirements
- Escalation procedures for retention questions

Technical Team:

- Detailed training on deletion procedures
- System administration for retention configuration
- Incident response for failed deletions

Customer-Facing Team:

- Customer retention option explanations
- Deletion request handling procedures
- Legal hold coordination processes

11.2 Customer Education

Resources Provided:

- Retention policy documentation
- Best practice guidelines
- Configuration tutorials
- Compliance requirement guidance

12. POLICY GOVERNANCE

12.1 Review and Updates

Annual Policy Review:

- Legal requirement changes
- Customer feedback integration
- Technical capability updates
- Industry best practice alignment

Quarterly Procedure Review:

- Deletion success rates
- Customer satisfaction with retention options
- System performance optimization
- Process efficiency improvements

12.2 Approval and Communication

Policy Changes:

- Legal and compliance team review
- Technical feasibility assessment
- Customer impact analysis
- 30-day advance notice for material changes

12.3 Record Keeping

Policy Documentation:

- Version control and change history
- Approval records and justifications
- Training completion records
- Compliance audit evidence

CONTACT INFORMATION

Data Protection Officer: markus@itsconvo.com

Technical Support: markus@itsconvo.com

Legal Inquiries: ivan@itsconvo.com

DOCUMENT CONTROL

- **Created:** August 29th, 2025
- **Last Reviewed:** September 1st, 2025
- **Next Review:** September 2026
- **Approved By:** Markus Kellermann, CEO

This policy should be reviewed by qualified legal and compliance professionals. Regular updates ensure alignment with evolving legal requirements and business needs.