Testing and Verification Procedures

Overview

This document describes testing and verification procedures that PRIVO auditors can use to verify COPPA compliance for both Storytailor (our web platform) and Story Intelligence™ (our future AI engine). All procedures are designed to be performed without access to internal source code or proprietary technical documentation.

Both products share the same COPPA infrastructure, so testing procedures apply to both.

Verification Approach

PRIVO auditors can verify COPPA compliance through:

1. **API Testing** - Test compliance endpoints directly
2. **Documentation Review** - Review policies and procedures
3. **Process Verification** - Verify workflows and data handling
4. **Compliance Monitoring** - Review audit logs and compliance reports

Age Verification Testing

Test Procedure 1: Adult Registration

Purpose: Verify that users 13 and older are not subject to COPPA protections.

Test Steps: 1. Register a new user with age 35 2. Verify registration succeeds 3. Verify COPPA protection flag is set to false 4. Verify no parent email is required 5. Verify no consent is required

Expected Results: - Registration succeeds - `isCoppaProtected: false` - `requiresConsent: false` - No parent email required

Test Procedure 2: Child Registration with Parent Email

Purpose: Verify that users under 13 require parent email and COPPA protection.

Test Steps: 1. Register a new user with age 8 2. Provide parent email address 3. Verify registration succeeds 4. Verify COPPA protection flag is set to true 5. Verify consent is required

Expected Results: - Registration succeeds - `isCoppaProtected: true` - `requiresConsent: true` - Parent email accepted

Test Procedure 3: Child Registration without Parent Email

Purpose: Verify that registration is rejected when parent email is missing for users under 13.

Test Steps: 1. Attempt to register a new user with age 10 2. Do NOT provide parent email address 3. Verify registration is rejected 4. Verify error message indicates parent email is required

Expected Results: - Registration fails - Error message: “Children under 13 require parent email for COPPA compliance” - Error code: “PARENT_EMAIL_REQUIRED”

Parental Consent Testing

Test Procedure 4: Consent Request Creation

Purpose: Verify that consent requests can be created for children under 13.

Test Steps: 1. Create a consent request with parent email and child age 2. Verify consent request is created 3. Verify unique request ID is generated 4. Verify status is set to “pending” 5. Verify expiration date is set (7 days from creation)

Expected Results: - Consent request created successfully - Unique request ID returned - Status: “pending” - Expiration date set correctly

Test Procedure 5: Consent Verification

Purpose: Verify that parents can verify consent.

Test Steps: 1. Use consent request ID from Test Procedure 4 2. Submit consent verification 3. Verify consent status changes to “verified” 4. Verify consent timestamp is recorded 5. Verify parent receives confirmation

Expected Results: - Consent verification succeeds - Status changes to “verified” - Consent timestamp recorded - Confirmation sent to parent

Test Procedure 6: Consent Status Check

Purpose: Verify that consent status can be checked at any time.

Test Steps: 1. Check consent status for a user 2. Verify current status is returned 3. Verify consent metadata is included (if available) 4. Verify consent history is accessible

Expected Results: - Consent status returned - Status values: “none”, “pending”, “verified”, or “revoked” - Metadata included when available

Test Procedure 7: Consent Revocation

Purpose: Verify that parents can revoke consent at any time.

Test Steps: 1. Revoke consent for a user with verified consent 2. Verify consent status changes to “revoked” 3. Verify data collection stops immediately 4. Verify revocation is logged 5. Verify parent receives confirmation

Expected Results: - Consent revocation succeeds - Status changes to “revoked” - Data collection stops - Revocation logged - Confirmation sent to parent

Parental Rights Testing

Test Procedure 8: Data Access Request

Purpose: Verify that parents can access all data about their child.

Test Steps: 1. Submit data access request as parent 2. Verify parent identity is validated 3. Verify all child data is returned 4. Verify data includes: user data, stories, characters, emotions, consent records 5. Verify response is provided within 30 days

Expected Results: - Data access request succeeds - All child data returned - Data in machine-readable format (JSON) - Response within 30 days

Test Procedure 9: Data Deletion Request

Purpose: Verify that parents can request deletion of all child data.

Test Steps: 1. Submit data deletion request as parent 2. Verify parent identity is validated 3. Verify all child data is deleted 4. Verify audit logs are anonymized (not deleted) 5. Verify parent receives confirmation

Expected Results: - Data deletion succeeds - All child data permanently deleted - Audit logs anonymized (retained for legal compliance) - Confirmation sent to parent

Test Procedure 10: Data Export Request

Purpose: Verify that parents can export all child data.

Test Steps: 1. Submit data export request as parent 2. Verify parent identity is validated 3. Verify export file is generated 4. Verify export includes all data types 5. Verify secure download link is provided (expires in 7 days)

Expected Results: - Data export succeeds - Export file in JSON format - All data types included - Secure download link provided - Link expires after 7 days

Data Retention Testing

Test Procedure 11: Automated Deletion Verification

Purpose: Verify that data is automatically deleted according to retention policies.

Test Steps: 1. Review data retention policies 2. Verify automated deletion processes are in place 3. Verify deletion occurs when retention period expires 4. Verify deletion is logged 5. Verify different deletion strategies (hard delete vs. anonymization)

Expected Results: - Retention policies documented - Automated deletion processes operational - Deletion occurs automatically - Deletion logged for audit - Appropriate deletion strategy applied

Security Testing

Test Procedure 12: Encryption Verification

Purpose: Verify that data is encrypted at rest and in transit.

Test Steps: 1. Verify database encryption is enabled 2. Verify API communications use HTTPS/TLS 3. Verify email delivery uses TLS encryption 4. Verify encryption keys are managed securely

Expected Results: - Encryption at rest enabled - Encryption in transit (TLS 1.3) required - Secure key management

Test Procedure 13: Access Control Verification

Purpose: Verify that access controls are properly implemented.

Test Steps: 1. Verify Row Level Security (RLS) is enabled 2. Verify users can only access their own data 3. Verify parents can only access their own child's data 4. Verify authentication is required for all API endpoints 5. Verify parent-child relationship verification

Expected Results: - RLS policies enforced - User-based access control - Parent-child relationship verified - Authentication required

Audit Logging Verification

Test Procedure 14: Audit Log Review

Purpose: Verify that compliance events are properly logged.

Test Steps: 1. Review audit log structure 2. Verify consent events are logged 3. Verify data access events are logged 4. Verify data deletion events are logged 5. Verify security events are logged 6. Verify log retention period (7 years)

Expected Results: - Audit logs comprehensive - All compliance events logged - Logs retained for 7 years - Logs anonymized after 1 year

Compliance Monitoring

Ongoing Monitoring Procedures

For PRIVO Auditors:

1. **Consent Status Monitoring:**
    - Review consent status reports
    - Verify consent rates and trends
    - Identify any compliance issues
2. **Data Retention Monitoring:**
    - Review data retention compliance reports
    - Verify automated deletion is working
    - Verify retention periods are being followed
3. **Parental Rights Monitoring:**
    - Review parental rights request summaries
    - Verify response times (within 30 days)
    - Verify all requests are properly handled
4. **Security Monitoring:**
    - Review security incident summaries
    - Verify incident response procedures
    - Verify security measures are effective

Test Environment

API Base URL: Available upon request for PRIVO audit
Test Credentials: Available upon request for PRIVO audit
Documentation: All API documentation available upon request

Contact Information

Privacy Inquiries: privacy@storytailor.com
Technical Contact: tech@storytailor.com
Mailing Address:
Storytailor Inc.
7131 w 135th, #1074
Overland Park, KS 66223

Response Time: All verification requests responded to within 30 days.

Storytailor Inc.
7131 w 135th, #1074
Overland Park, KS 66223