Third-Party Services

Overview

This document provides compliance documentation for all third-party services used by both Storytailor (our web platform) and Story Intelligence™ (our future AI engine). All services have publicly available Data Processing Agreements (DPAs) and compliance documentation that can be referenced for PRIVO certification.

Approach: We reference publicly available compliance documentation from each service provider rather than including full DPAs in this package. All DPAs are available on the respective service provider websites.

AWS Services

Services Used

- **AWS Lambda:** Serverless function execution for platform operations
- **AWS SSM Parameter Store:** Secure storage for secrets and configuration
- **AWS S3:** Asset storage for stories, images, and audio files
- **AWS EventBridge:** Event-driven communication between services
- **AWS CloudWatch:** Logging and monitoring

Compliance Documentation

Data Processing Addendum (DPA): - **Status:** Automatically applies to all AWS customers globally - **Location:** Incorporated into AWS Service Terms - **Reference:** https://aws.amazon.com/service-terms/ - **Note:** The AWS DPA is automatically incorporated into the AWS Service Terms and applies to all customers globally who require it to comply with GDPR when using AWS services to process personal data.

COPPA Support: - AWS services can be configured to support COPPA compliance - **Amazon Lex:** Supports `childDirected` flag to indicate COPPA compliance - **Reference:** https://docs.aws.amazon.com/lexv2/latest/APIReference/API_DataPrivacy.html - **Note:** When using Amazon Lex, setting `childDirected` to `true` indicates that your application is subject to COPPA, and Amazon Lex will handle data accordingly.

Compliance Programs: - AWS maintains multiple compliance certifications - **Reference:** https://aws.amazon.com/compliance/ - **Certifications Include:** - SOC 2 Type 2 - ISO 27001 - HIPAA - PCI DSS - And many more

Data Protection Measures

Encryption: - **At Rest:** S3 buckets encrypted, SSM parameters encrypted with AWS KMS - **In Transit:** All AWS API calls use HTTPS/TLS - **KMS:** AWS Key Management Service for encryption key management

Access Control: - **IAM Roles:** Lambda functions use IAM roles with least privilege - **S3 Policies:** S3 buckets protected by IAM policies - **SSM Encryption:** All SecureString parameters encrypted with AWS KMS

Data Residency: - Configurable data residency options - Data stored in specified AWS regions - **Current Region:** us-east-1 (United States)

Log Retention: - CloudWatch logs retained per retention policy (typically 30 days) - Configurable retention periods

Data Flow

Data Stored in AWS: - **Lambda Logs:** May contain user IDs, session IDs, story content (CloudWatch Logs) - **SSM Parameters:** API keys, secrets (no user data) - **S3 Buckets:** Story assets, images, audio files (may contain child-created content) - **EventBridge Events:** Event data (may contain user IDs, session IDs)

Data Minimization: - Only necessary data stored in AWS services - Logs contain minimal PII (user IDs, not full user data) - S3 assets contain user-created content (stories, images, audio)

Compliance Status

COPPA Compliance: AWS provides encryption, access control, and supports our retention policies
GDPR Compliance: Includes encryption, access control, and data minimization features
Shared Responsibility: We're responsible for how we use the services; AWS is responsible for the infrastructure security

Privacy Risk Assessment: - **Risk Level:** Low (AWS provides enterprise-grade security) - **Mitigation:** Encryption, access control, retention policies, IAM roles - **Parental Consent:** Required for children under 13 (data stored in AWS services)

Supabase

Services Used

- **PostgreSQL Database:** Primary data storage for all user data
- **Authentication Service:** User authentication and account management
- **Row Level Security (RLS):** Database-level access control

Compliance Documentation

Data Processing Addendum (DPA): - **Status:** Available for all Supabase customers - **Location:** https://supabase.com/legal/dpa - **Process:** DPA can be made legally binding by signing and completing details through a PandaDoc document prepared by Supabase - **Reference:** Request DPA from the legal documents page of your Supabase dashboard

HIPAA Compliance: - Supabase offers HIPAA-compliant environments - **Reference:** https://supabase.com/docs/guides/security/hipaa-compliance - **Note:** While Supabase offers HIPAA compliance, COPPA compliance is the customer's responsibility

Security Certifications: - **SOC 2 Type 2:** Certified - **Reference:** https://supabase.com/security - **Security Page:** https://supabase.com/security

COPPA Compliance: - **Status:** Customer responsibility - **Note:** Supabase does not provide specific COPPA documentation. COPPA compliance is the customer's responsibility. Supabase provides security and compliance features (SOC 2, HIPAA) that support COPPA compliance.

Data Protection Measures

Encryption: - **At Rest:** Database encryption enabled - **In Transit:** SSL/TLS required for all connections - **Reference:** Supabase automatically encrypts data at rest and requires SSL/TLS for all connections

Row Level Security (RLS): - **Status:** Enabled on all tables - **Implementation:** User-based access control policies - **COPPA Protection:** RLS policies enforce COPPA-protected user restrictions

Data Residency: - Configurable data residency options - Data stored in specified regions - **Current Region:** United States

Backup & Recovery: - Automated backups - Point-in-time recovery available - **Reference:** Supabase provides automated backup and recovery services

Data Flow

Data Stored in Supabase:

Current (Storytailor 3.0): - **User Accounts:** User IDs, emails, ages, parent emails - **Story Content:** Stories created by children - **Character Data:** Characters created by children - **Parental Consents:** Parent consent records - **Safety Incidents:** Safety incident logs (content hashed, not raw text)

Future (Story Intelligence™): - **Emotional Data:** Emotion tracking data (365-day retention) - **Audio Transcripts:** Voice conversation transcripts (30-day retention) - **Conversation States:** Conversation session data (24-hour retention)

Data Protection Measures: 1. **Row Level Security (RLS):** All tables protected by RLS policies 2. **Encryption at Rest:** Supabase provides encryption at rest 3. **Encrypted Transmission:** All database connections use SSL/TLS 4. **Data Retention:** Automated

retention policies for all data types 5. **COPPA Protection:** Automatic COPPA protection flags for users under 13 6. **Parental Consent:** Parent consent required for children under 13 7. **Access Control:** Service role key used only for server-side operations 8. **Anonymization:** Emotional data anonymized after 365 days (not deleted) 9. **Content Hashing:** Safety incidents store content hashes, not raw text

Compliance Status

COPPA Compliance: Supports Row Level Security, parental consent workflows, and data retention policies
GDPR Compliance: Includes data retention, right to erasure, and encryption features
Data Minimization: We only store what's necessary for the service to work

Privacy Risk Assessment: - **Risk Level:** Low (data stored securely with RLS and encryption) - **Mitigation:** RLS policies, encryption, retention policies, parental consent - **Parental Consent:** Required for children under 13

SendGrid (Twilio)

Services Used

- **Email Delivery:** Parent notifications, transactional emails
- **Email Tracking:** Open and click tracking (optional)

Compliance Documentation

HIPAA Compliance: - SendGrid offers HIPAA-compliant email services - **Reference:** https://support.sendgrid.com/hc/en-us/articles/360041790233-Is-Twilio-SendGrid-HIPAA-Compliant - **Note:** HIPAA compliance available for enterprise customers

Email Compliance: - SendGrid complies with email opt-in/opt-out requirements - **Reference:** https://support.sendgrid.com/hc/en-us/articles/4404315959835-Email-Opt-in-and-Opt-out-Requirements - **CAN-SPAM Compliance:** SendGrid helps customers comply with CAN-SPAM Act

COPPA Compliance: - **Status:** Customer responsibility - **Note:** SendGrid does not provide specific COPPA documentation. COPPA compliance is the customer's responsibility. SendGrid provides email delivery services that can be used in a COPPA-compliant manner.

Data Processing Agreement: - **Status:** Available through Twilio's legal documentation - **Reference:** Contact Twilio support for DPA information - **Note:** SendGrid is a Twilio service, so DPAs are managed through Twilio

Data Protection Measures

Encryption: - **In Transit:** TLS encryption for email delivery - **Reference:** All email delivery uses TLS encryption

Data Minimization: - **Parent Email Only:** Only parent email addresses sent (not child emails) - **Content Minimization:** Email content limited to necessary information - **No PII in Headers:** User IDs and other PII not included in email headers

Purpose Limitation: - Emails sent only for notifications and transactional purposes - No marketing emails sent to parents - No child data included in emails

API Key Security: - SendGrid API keys stored securely in AWS SSM Parameter Store - Keys encrypted and access-controlled

Data Flow

Data Sent to SendGrid: - **Parent Email Addresses:** Sent (for parent notifications) - **Email Content:** Sent (notification text, safety alerts) - **User ID:** Not sent (only email addresses) - **Child Age:** Not sent (only in email content if relevant to notification) - **Story Content:** Not sent (only safety incident summaries) - **Child Name:** Not sent (only generic references like "your child")

Data Protection Measures: 1. **Parent Email Only:** Only parent email addresses sent (not child emails) 2. **Content Minimization:** Email content limited to necessary information 3. **No PII in Headers:** User IDs and other PII not included in email headers 4. **Encrypted Transmission:** All email delivery uses TLS encryption 5. **API Key Security:** SendGrid API keys stored securely 6. **Purpose Limitation:** Emails sent only for notifications and transactional purposes

Compliance Status

COPPA Compliance: Supports data minimization, encryption, and purpose limitation
GDPR Compliance: Includes data minimization, encryption, and purpose limitation
CAN-SPAM Compliance: Provides opt-in and opt-out support

Privacy Risk Assessment: - **Risk Level:** Low (only parent emails sent, minimal data) - **Mitigation:** Data minimization, encryption, purpose limitation - **Parental Consent:** Required for children under 13 (parent emails used for notifications)

Data Processing Agreements Summary

Agreement Status

Service Provider	DPA Available	Location	Status
AWS	Yes	Automatically applies (AWS Service Terms)	Active

Service Provider	DPA Available	Location	Status
Supabase	Yes	https://supabase.com/legal/dpa	Available for signing
SendGrid (Twilio)	Yes	Through Twilio legal documentation	Available upon request

DPA References

For PRIVO Certification: - All third-party services have publicly available Data Processing Agreements - DPAs can be referenced rather than included in this package - All DPAs are available on the respective service provider websites

Public Compliance Documentation Links

AWS

- **Compliance Programs:** https://aws.amazon.com/compliance/
- **Service Terms (includes DPA):** https://aws.amazon.com/service-terms/
- **COPPA Support (Lex):** https://docs.aws.amazon.com/lexv2/latest/APIReference/API_DataPrivacy.html

Supabase

- **Data Processing Addendum:** https://supabase.com/legal/dpa
- **Security:** https://supabase.com/security
- **HIPAA Compliance:** https://supabase.com/docs/guides/security/hipaa-compliance

SendGrid (Twilio)

- **HIPAA Compliance:** https://support.sendgrid.com/hc/en-us/articles/360041790233-Is-Twilio-SendGrid-HIPAA-Compliant
- **Email Compliance:** https://support.sendgrid.com/hc/en-us/articles/4404315959835-Email-Opt-in-and-Opt-out-Requirements
- **Twilio Legal:** Contact Twilio support for DPA information

Contact Information

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

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