Wyng Tech Guide:

Consumer Data Collection and End-to-End Data Flow

Purpose

This guide summarizes how Wyng collects, processes, and delivers customer data on behalf of our clients. This covers the end-to-end data flow from collection and onboarding, processing, and delivery of data and events to downstream systems like data clouds, CDPs, marketing automation, loyalty, and custom endpoints.

The guide also reviews onboarding of segments, loyalty tiers, transaction history, and other customer attributes relevant for personalization and progressive profiling. Capabilities providing control of quality, integrity, and security while collecting customer data will also be discussed. The goal is to help marketing and technology teams understand how Wyng can plug into their tech stack, and plan data flows that are reliable, scalable, and easy to maintain.

In this guide:

1. Consumer Data Collection
2. Security & Compartmentalization
3. Compliance
4. Data Flow Diagram
5. Controlling Data Quality & Integrity
6. Inbound Data Integration
7. Outbound Data Integration

1. Consumer Data Collection

Wyng offers flexible, secure methods for collecting first-party data (1PD) and zero-party data (ZPD) at any point in the customer journey — from forms embedded in promotions and games, to quizzes on websites or ecommerce pages, to seamless collection from any web or mobile application via APIs/SDKs.

These methods include configurable and customizable form embeds and quiz embeds, Experiences SDK, Profiles SDK, and Profiles API. These mechanisms can be used to collect new data from customers during a web or mobile app user session, and also to onboard known IDs, attributes, and data programmatically from web or application session context. Programmatic methods are described further in the "Data Integration - Input to Wyng" section.

2. Security & Compartmentalization

Wyng platform includes multiple layers of safeguards to secure data collection and give clients control over how data is isolated for different teams and business units.

Wyng adopts a multi-layer approach to security that includes partnership with market leading cloud data center partners, minimal public network footprint, use of private subnets for production hosts and datastores, intrusion detection and intrusion prevention systems across all production hosts, managed web application firewall, centrally managed anti-malware across all hosts, and automated weekly web application vulnerability scans.

Encryption

Independent of source and method, all data collected by or onboarded into Wyng is encrypted in-transit and at-rest using best practice algorithms and keys, and processed and hosted within an isolated logical compartment of our multi-tenant system. Each client retains sole ownership of all data collected and processed by their use of the platform.

Accounts and sub-accounts - Wyng Properties

Each Wyng client has an umbrella account, which handles user identification and authentication including SSO integration with a client's IdP, and contains one or more sub-accounts for different teams. Wyng sub-accounts are called "Properties". Each Property is an isolated logical compartment for Wyng experiences, assets, customer data, and metrics. A client can choose how many Properties to set up, who should have access to each, and with what roles: for example, separate Properties might be set up for brand or market teams, business units, or for agencies using Wyng, customer account teams.

All data collection, processing, and hosting happens within a Property. Access to a Property is limited to a list of users who have been authorized with specific roles for that Property. API credentials are also scoped by Property: e.g. an API access token for Property A will not provide access to data in Property B in the same client account.

Properties may be added to or removed from a client account in accordance with the terms of the governing license agreement with the client. Experiences and templates may be copied from one Wyng property to another. Data can be exported from a property by users with the required privileges; however, collected data cannot be moved or copied from one Wyng Property to another.

3. Compliance

Wyng undertakes an annual SOC 2 Type II audit to assess and confirm alignment with trust services criteria related to Security, Availability, and Confidentiality. The audit process includes understanding Wyng service commitments and system requirements, assessing controls to confirm they are suitably designed and operate effectively, obtaining sufficient evidence to confirm the descriptions of controls and the effectiveness of the controls, and thoroughly testing the operating effectiveness of the controls to provide reasonable assurance that Wyng achieved its service commitments in accordance to the applicable trust services criteria.

Security audits

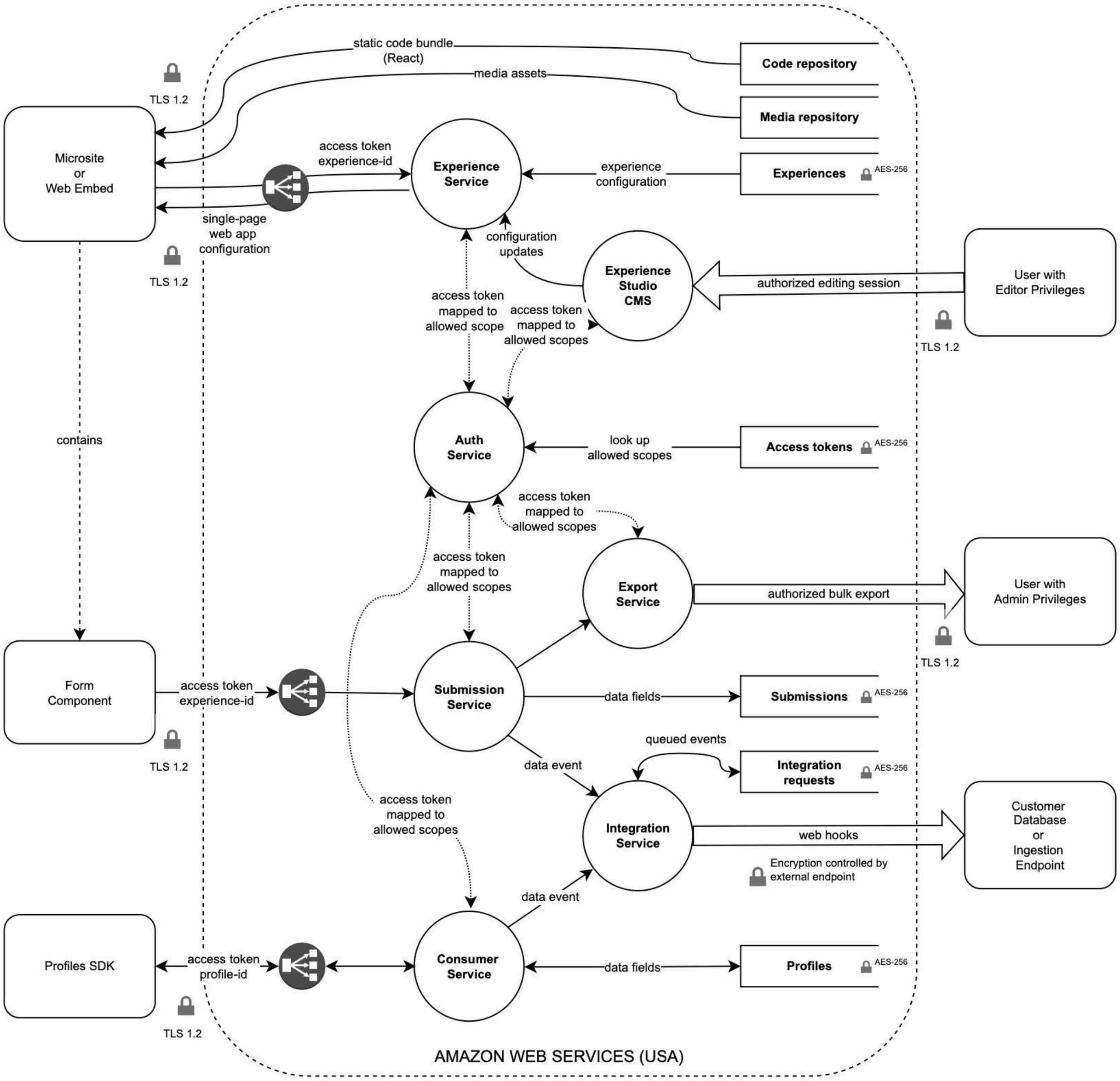
As a key compliance control, Wyng undertakes an annual in-depth security audit in partnership with a third-party security specialist. The scope of the test includes external "black box" penetration testing, comprehensive "white box" penetration testing from within the private network, and manual+automated web application vulnerability scanning. Any vulnerabilities identified during these tests are classified by risk, and remediated on a timetable defined by risk category. To ensure a diversity of testing patterns, Wyng periodically rotates between security specialist firms.

Additionally, Wyng internally assesses compliance with HIPAA, WCAG 2.1 level AA, GDPR, PIPEDA, CCPA, and emerging privacy regulations at the state level in the U.S.A.

Data Subject Requests

Wyng implements an always-on process for handling Data Subject Requests from Wyng clients and individuals, to search for, retrieve, and/or delete the personal data of individuals processed. Clients and individuals may address any DSRs to privacy@wyng.com to initiate a request, which enters our privacy process, and is tracked and handled promptly. Clients who use OneTrust governance/risk/compliance software can directly integrate their OneTrust instance with the Wyng privacy process. Finally, Wyng offers a market leading Privacy Dashboard to clients, where users with appropriate privileges can initiate DSRs and track to completion, on a self-service basis. A declaration of Wyng's DSR process and other relevant policy commitments can be found in Wyng's Privacy Policy, here: https://www.wyng.com/privacy-policy/

4. Data Flow Diagram



COMPONENT	TYPE	PURPOSE
Experience Service	API	Configuration and generation of experiences with data collection elements.
Experience Studio CMS	App	Web application for users to design and deploy experiences.
Auth Service	API	Access tokens for users and API clients.
Submission Service	API	Incoming data from user interaction with forms and quizzes.
Consumer Service	API	Persistent user profiles for personalization and progressive data collection.
Integration Service	API	Outbound data event stream from Wyng to client systems.
Export Service	API	Batch export of data from Wyng to files.

5. Controlling Data Quality & Integrity

Wyng provides clients with comprehensive and flexible controls over data quality and integrity.

Field validation

Wyng form and quiz embeds include robust and customizable field validation (required fields, format checks, word or character limits, custom rules, and more) to ensure data collected is usable and of needed quality and completeness.

Identity verification

For enrichment, loyalty, personalization, and other touch points requiring a persistent user identity across sessions, Wyng integrates with your existing user authentication systems, like website login or loyalty app login. For cases where no existing user login mechanism exists, Wyng includes built-in, one-click email identity verification and mobile phone number (SMS) verification using One-Time Passwords so brands can validate provided IDs before allowing participation and collecting data. For cases where personalized outbound messages (email, SMS, or WhatsApp) include click-through links, Wyng can automatically pull user identification tokens (e.g. hashed email address) from URL parameters, to facilitate immediate personalization of landing pages, including display of varying content to users based on segments.

Fraud prevention and mitigation

Wyng includes advanced controls to protect against fraud and unwanted traffic, including AI generated traffic, via proprietary Intelligent Bot Defense to identify and filter out bot activity without disrupting or adding friction to human interactions, an automated referrer blocklist to redirect low-quality traffic from sweepstakes aggregator sites and spammy sources, and country-gating to block or re-route traffic from users outside of targeted markets.

Unique invitation codes

For programs where participation should be limited to invited users, for example, via distribution of unique invitation codes on receipts, at events, on product packaging, as loyalty rewards, or as value exchange for repeat participation in digital experiences, Wyng has real-time, zero-code support for validation and consumption of unique invitation codes, as a pre-condition for access to a digital experience. This functionality is secure and scalable, supporting validation and redemption of tens of millions of unique codes, and the tracking of codes redeemed to individual participants. Further, for programs encouraging repeat participation across a series of promotions or sweeps, Invitation Codes can include tokenized chances to win–a flexible, innovative mechanism to encourage repeat participation over a series of related programs, with full automation of the winner selection process.

Participation policies

Wyng makes it easy to configure and automatically enforce a broad set of other participation policies including age-gating, geo-fencing, authentication-gating, individual submission limits, and total submission limits across all participants. Additionally, centralized privacy governance settings enable central control and enforcement of required privacy policies, consent, and terms.

6. Inbound Data Integration

Data can be programmatically onboarded into Wyng to append known user IDs to collected data, enable progressive data collection, support in-session or cross-session personalization, attach meta data for tagging and classification, track UTM parameters, and other use cases. Sources of data can include:

- Unique click-through links in personalized messages (email, SMS, WhatsApp)
- Tracking parameters in paid media click-throughs
- IDs and profile attributes for users logged into websites or mobile apps
- Mobile app device data
- Loyalty platform member IDs, loyalty tiers, loyalty points balances
- Transaction history from commerce platforms
- Segments from CDPs or website personalization systems
- Communication preferences from ESPs or preference centers

Once data has been onboarded to Wyng–either during a user session or in advance of user sessions–it can be leveraged immediately during the user session to enable progressive data collection or personalization of content or user flow.

Onboarding data by front-end integration

Data can be integrated by a variety of mechanisms during a user session on website, progressive web application, or mobile app:

- URL Parameters - datapoints such as user ID or hashed email
- Local and session storage - any first-party application data stored in the browser
- First-party cookies - Wyng dynamic embeds have full access to first-party cookies
- HTTP Headers - convenient for passing IDs and fields from native mobile apps
- Pull API calls - data can be pulled from an endpoint at any point in a session
- Wyng JS SDK - IDs, attributes, and meta data can be set in hidden form fields

- Wyng Profiles SDK - IDs, attributes, and any user data can be persisted on the back-end, in real-time, for use in this user session and future user sessions

Onboarding data by back-end integration

In addition, user profile data including IDs, attributes, segments, transaction history, loyalty tiers, loyalty points, etc. can be onboarded in advance of user sessions by pushing data from any client system to Wyng, using Profiles API:

- Profiles API - push data in advance of user sessions

Pushing data to Wyng requires you to first set up a structured data model to receive and organize the fields you plan to send. To learn more, see Intro to Wyng Profiles.

Wyng Profiles for cross-session personalization

Data onboarded to Wyng Profiles can be used for personalization across all future Wyng sessions with that user. Collected attributes can be associated with anonymous or known user IDs and stored persistently for real-time access during future user sessions. Segments can be defined using flexible rules and criteria, and used in real-time for progressive data capture or content personalization.

In addition to being used for cross-session personalization of Wyng experiences, user profiles and segments in Wyng Profiles can add real-time personalization to any web app or mobile app, using Profiles SDK and API. The security model permits embedding public access tokens in front-end code, while preserving full security of the personal data in the profile. For applications where a user's identity is authenticated, the security model permits trusted delivery of a user-scoped JWT to the front-end, to permit temporary secure access to the private data in a specific profile.

Using Wyng Profiles for cross-session personalization requires you to first set up a structured data model. To learn more, see Intro to Wyng Profiles.

7. Outbound Data Integration

Wyng can stream data and events from user sessions to third-party or client systems to enable timely triggered follow ups, in-session personalization, and real-time 360 degree views.

Wyng provides a variety of connectors for delivering data and events from user sessions:

- Wyng Webhook is a general purpose connector that can securely send data with customized authentication and payloads to any REST API endpoint including CDPs, Loyalty platforms, CRMs, and enterprise data integration platforms like MuleSoft.

- Wyng connects directly to Snowflake and other cloud-based data platforms by streaming data in semi-structured (JSON) format to S3 buckets or GCS buckets.
- Wyng has plug-in connectors to many leading Martech systems, including Braze, Attentive, Klaviyo, Segment, Qualtrics, Epsilon, Salesforce, Acquia, Eloqua, Responsys, Voucherify, and Mailchimp.
- On client request, Wyng can add custom plug-in connectors to internal enterprise systems, third-party systems, or any API. These are developed in a priority roadmap track, concurrent with account onboarding.

Transactions can be triggered by a variety of user-related events processed by Wyng:

- Data collected by a specific form or quiz
- Data collected across all forms (Property-wide integration)
- Creation and/or updates to persistent user profiles in Wyng
- Submissions and/or moderation of UGC photos or videos (User Generated Content)
- @mentions or use of brand #hashtags on Instagram

The Integrations dashboard in Wyng provides a rich set of monitoring and management tools for data and event streams, including:

- Backfill of historical data: Add a connector after an experience has started collecting data to automatically catch up, without any data loss
- Auto-retry of failed transaction attempts
- Email notifications on repeated failure
- Manual requeue and retry of failed transactions
- Real-time transaction logs including failure codes
- Concurrent and simultaneous outbound streams to multiple systems

Transaction security

Transactions are delivered securely, via server-to-endpoint authenticated connections. A variety of auth and security options are supported including OAuth with credential refresh, auth headers, IP whitelists, and any required system-specific auth mechanisms for plug-in connectors.

Data retention

In most cases data is retained in Wyng after delivery to an external system. However, clients with restrictive PII storage policies can automatically delete personal data from Wyng after it has been successfully transferred to an external system. This minimizes the footprint of data in Wyng to the small window of time between the start of a user session and completion of a successful data transfer to the external system.

Batch exports

While real-time connectors for outbound data flows are strongly encouraged for all Wyng clients, in cases where a client is unable or not ready to accept real-time data flow, comprehensive batch data exports are available for all data collected by Wyng experiences.