

Title: How Our App Uses Platform Data

Table of Contents

1. Executive Summary
2. Legal Basis and Compliance
3. Data Categories Collected
4. Data Flows and Processing
5. Storage, Retention, and Deletion
6. Security and Access Controls
7. User Rights and Consent Management
8. Data Sharing and Transfers
9. Data Governance and Roles
10. Lifecycle and Change Management
11. Appendices (Glossary, Data Elements Dictionary, Contacts)

1. Executive Summary

- Purpose: This document describes how our app collects, processes, stores, and deletes Platform Data to deliver services, ensure security, and drive product improvements.
- Scope: Applies to all users, partners, and internal systems involved in data handling for the app.

2. Legal Basis and Compliance

- Purposes: List the legitimate purposes (e.g., service delivery, authentication, security, fraud prevention, analytics, personalization, product improvement).
- Legal Basis: For each data category, specify the legal basis (contract performance, legitimate interests, consent, legal obligation, etc.).
- Regulatory Context: GDPR, CCPA, other applicable laws; explain how requirements are met (data minimization, purpose limitation, rights, and retention).

3. Data Categories Collected

For each category, provide: description, source, processing, retention, and example data elements.

- Account/Identity Data

- Source: User input, authentication services

- Processing: Authentication, access control, personalization
- Retention: as per policy (e.g., 2 years after last activity or per contract)
- Elements: user_id, email, username, profile attributes

- Usage and Interaction Data

- Source: App events, logs
- Processing: Feature usage analytics, anomaly detection
- Retention: per policy (e.g., 12–24 months)
- Elements: event_id, timestamp, action, page, device type

- Device and Network Data

- Source: Devices, network headers
- Processing: Security checks, compatibility assessments
- Retention: per policy
- Elements: IP address, device_id, OS version

- Content and Communications Data

- Source: User-provided content, messages
- Processing: Moderation, search indexing, feedback analysis
- Retention: per policy
- Elements: content_text, metadata, attachments (where applicable)

- Location Data

- Source: Geolocation (approximate)
- Processing: Regional features, risk assessment
- Retention: per policy
- Elements: geolocation_coordinates or region

- Analytics and Model Data

- Source: Aggregated/apply data from usage
- Processing: Aggregation, model training, performance measurement
- Retention: aggregated/anonymized long-term storage
- Elements: aggregated_metrics, anonymized_user_ids (pseudonymized)

4. Data Flows and Processing

- Ingestion: How data enters the system (frontend, APIs, integrations)
- Processing: Validation, normalization, enrichment, and transformation steps
- Storage: Primary databases, data lakes, caches, backups
- Access Control: Roles, permissions, and least-privilege principle
- Sharing: With partners or third-party services, purposes, safeguards
- Retention and Deletion: Retention periods, deletion triggers, and deletion methods
- De-Identification: Anonymization/pseudonymization where applicable

5. Storage, Retention, and Deletion

- Data Stores: List of data stores and their purpose
- Retention Schedules: Per data category and data element
- Deletion Procedures: Immediate deletion vs. scheduled purge; handling backups
- Legal Holds: Process for holds and resumption of deletion

6. Security and Access Controls

- Data in Transit: TLS/HTTPS, VPN where applicable
- Data at Rest: Encryption (e.g., AES-256)
- Access Management: Role-based access control, multi-factor authentication
- Logging and Monitoring: Audit trails, anomaly detection, alerting
- Data Integrity and Backups: Versioning, backup retention, disaster recovery

7. User Rights and Consent Management

- Access and Portability: How users can view and export data
- Correction and Deletion: Procedures to correct or delete data
- Consent: How consent is captured, stored, and withdrawn
- Preferences: How users manage data preferences and opt-outs