



CODA App Policies

CODA: Live Forever

Status: Legal and product review draft — do not publish yet

Prepared from the product implementation reviewed on: 22 September 2026

Proposed effective date: [EFFECTIVE DATE]

Controller: [FULL LEGAL ENTITY NAME], [REGISTERED ADDRESS AND COUNTRY]

This document contains a combined Privacy Policy, Terms of Service, Acceptable Use Policy, Cookie Notice, and regional privacy addendum for **CODA: Live Forever** (the “Service”). It is based on the current mobile app, website, backend, and administration features. It is a practical draft, not legal advice or a substitute for review by counsel in each launch country.

Before publication, replace every [BRACKETED ITEM], approve the proposed retention schedule, and complete the release blockers in the final section.

Document contents

Part I Privacy Policy

Part II Terms of Service

Part III Acceptable Use Policy

Part IV Regional Privacy Addendum

Part V Internal Release Requirements

Product scope used for this draft

CODA currently supports:

- account creation using a name, phone number, optional or required email address, password, and SMS or email verification;
- private memory titles, text, photos, videos, audio, PDFs, Word documents, and related file metadata;
- recipients entered by the user, including their name, email address, and optional phone number;
- delivery at a scheduled date or after an overdue activity check-in;
- recipient account matching and access to assigned memories;
- activity check-ins, local and remote reminders, and notification delivery by push, email, or SMS;
- paid subscriptions through Apple, Google Play, and Stripe, plus a non-renewing basic trial;
- secure account sessions, subscription usage limits, file preview/download, and administrative operations; and
- a public website and authenticated web account/billing area.

CODA does **not** currently use advertising SDKs, behavioral advertising, a mobile analytics SDK, contact-book access, or device location APIs. If any of these practices change, this policy and the store disclosures must be updated before release.

PART I

Privacy Policy

1. Who we are

[FULL LEGAL ENTITY NAME] (“CODA,” “we,” “us,” or “our”) operates CODA: Live Forever and is the controller or responsible party for personal data processed through the Service.

Contact details:

- Registered address: [FULL REGISTERED ADDRESS]
- Privacy email: [PRIVACY EMAIL — RECOMMENDED: privacy@codaliveforever.com]
- Support email: [SUPPORT EMAIL]
- Data Protection Officer, if appointed: [DPO NAME OR CONTACT]
- EU representative, if required: [EU REPRESENTATIVE NAME, POSTAL ADDRESS, EMAIL]
- Other local representative or Information Officer, if required: [DETAILS BY COUNTRY]

2. Scope

This Privacy Policy applies to the CODA iOS and Android apps, the CODA website and web account, related communications, customer support, and backend services. It does not govern third-party services that users access under separate terms, such as the Apple App Store, Google Play, or Stripe-hosted payment pages.

3. Personal data we process

3.1 Account and profile data

We process:

- name;
- phone number;
- email address, when supplied or required;
- preferred language;
- password in hashed form;
- account and verification status;
- account creation and update dates; and
- session and device information supplied during login, such as an optional device description.

3.2 Memory content

At the user’s direction, we process:

- memory titles and written messages;
- photos and videos;
- voice recordings and other audio;
- PDFs, Word documents, and other supported files;
- filenames, file type, size, and upload dates;
- selected recipients;
- scheduled delivery date, time, time zone, and trigger type; and
- memory status, delivery status, and view status.

Users choose the content they upload. It may incidentally contain personal or sensitive information about the user or another person. Users must not upload another person's information unless they have a lawful basis and authority to do so.

3.3 Recipient data supplied by another user

A CODA user may provide a recipient's:

- name;
- email address;
- phone number; and
- relationship to a memory, assignment, delivery, and view status.

We may match a recipient's normalized email address or phone number with an existing CODA account so that the intended recipient can securely receive an assigned memory. We do not import a user's address book.

3.4 Activity and check-in data

We process:

- check-in interval;
- check-in and response timestamps;
- reminder counts and reminder delivery state;
- whether a check-in is pending or overdue; and
- the date and time a recipient viewed a delivered memory.

This data is used to operate the user-selected delivery rule. CODA does not treat a missed check-in as verified evidence of death, incapacity, health status, or any legal event.

3.5 Subscription and transaction data

We process:

- plan, entitlements, quotas, trial status, and subscription status;
- store product, offer, and transaction identifiers;
- purchase and expiration dates;
- billing platform, amount, currency, and country or storefront code;
- hashed or encrypted provider purchase tokens and provider responses; and
- Stripe customer and subscription identifiers for web purchases.

Payment card or bank details entered on an Apple, Google, or Stripe payment surface are handled by that provider and are not received by CODA unless the provider separately makes limited transaction data available to us.

3.6 Device, notification, and technical data

We process:

- native push notification token and platform;
- IP address, request date/time, request path, response status, referrer, and user-agent information in server logs;
- authentication and refresh-token records;
- security and rate-limit events;
- local notification preferences and scheduling data stored on the device; and
- limited operational logs and error information generated by our servers.

We do not use an advertising identifier or track users across other companies' apps or websites.

3.7 Support and administration data

We process communications sent to support, actions taken by authorized administrators, account status changes, and audit records needed to operate, secure, and investigate the Service. The administration interface is designed to expose memory metadata and recipient/file metadata without exposing decrypted memory content.

4. Where the data comes from

We receive personal data:

- directly from users during signup, profile updates, content upload, recipient creation, check-ins, purchases, or support requests;
- from another user who designates a person as a recipient;
- from Apple, Google, or Stripe in connection with purchases and subscriptions;
- from a user's device and our servers when the Service is used; and
- from notification, email, SMS, storage, and infrastructure providers when they return delivery or operational status.

5. Why we process data and our legal bases

The legal basis depends on the country and context. For users in the EU/EEA, the proposed bases are:

Purpose	Data	Proposed legal basis
Create and secure an account	Account, verification, tokens, technical logs	Performance of a contract; legitimate interests in security and fraud prevention
Store, preview, download, and deliver memories	Memory content, files, schedules, recipient links	Performance of a contract and the user's instructions
Match and notify a recipient	Recipient contact data and assignment state	Legitimate interests in fulfilling the sender's requested private delivery, balanced against the recipient's rights; consent where local law requires it
Operate check-ins and reminders	Check-in history, push token, email/phone	Performance of a contract; consent or user choice for optional device permissions and communications where required
Manage subscriptions and purchases	Transaction and entitlement data	Performance of a contract; legal obligations; legitimate interests in reconciliation and fraud prevention
Provide support and improve reliability	Support content, operational events, logs	Performance of a contract; legitimate interests in support, debugging, and service improvement
Protect users and the Service	Logs, account and admin activity	Legitimate interests in security, abuse prevention, and enforcing our terms; legal obligations
Meet legal requirements	Relevant account, transaction, and audit records	Compliance with legal obligations and establishment, exercise, or defense of legal claims

We do not intentionally request special-category data such as medical information, religious beliefs, political opinions, or biometric identifiers. If a user chooses to include such information in private content, we process it only to provide storage and delivery at the user's direction and only where a valid condition under applicable law is available. Users must not include sensitive data about another person without appropriate authority or consent.

We do not use personal data for solely automated decisions that produce legal or similarly significant effects. Automated scheduling, check-in reminders, delivery eligibility, quota enforcement, and subscription reconciliation carry out user-selected or contractual rules and can be reviewed by support.

6. How memory encryption works

Memory text and uploaded files are encrypted at rest using AES-256-GCM before being stored. Network communications must use HTTPS/TLS in production. Authentication tokens are stored using platform-protected storage on supported devices, and passwords are stored as hashes.

CODA's current architecture is **not end-to-end encrypted** and must not be described as zero-knowledge, quantum-secure, or inaccessible to CODA. CODA servers hold the encryption capability and decrypt content when an authorized sender or recipient previews or downloads it. Access is limited by authentication, authorization, operational controls, and the purposes described in this policy.

No security method is perfect. Users should keep independent copies of irreplaceable content and should not use CODA as the only means of preserving or delivering legally or personally critical information.

7. When we disclose data

7.1 Chosen recipients

When a delivery condition is met, we make the selected memory available to the recipient account linked by the email address or phone number provided by the sender. Notification messages identify the sender and state that a CODA memory is available, but they do not include the memory content itself.

7.2 Service providers

Subject to final vendor and hosting confirmation, CODA uses or integrates with:

Provider/category	Data and purpose
[MYSQL/VPS/CLOUD HOST NAME AND REGION]	Application and database hosting
Cloudflare R2	Encrypted media and document storage
Twilio	SMS verification, reminders, and recipient notifications when enabled
Microsoft 365 / configured SMTP provider	Email verification, reminders, and recipient notifications
Apple Push Notification service	iOS push delivery
Google Firebase Cloud Messaging	Android push delivery
Apple App Store and Google Play	Mobile purchase processing, verification, subscription status, and refunds

Provider/category	Data and purpose
Stripe	Web checkout, billing portal, subscription status, and transaction records
Professional advisers and authorities	Legal, audit, security, compliance, and lawful requests

We require processors to protect personal data and use it only for authorized services. The final published policy must link to a current subprocessor list or name the actual providers and processing locations.

7.3 Legal, safety, and corporate events

We may disclose data when reasonably necessary to comply with law, enforce our terms, protect users or the public, investigate fraud or security incidents, or establish and defend legal claims. If our business is reorganized, financed, acquired, or sold, data may be transferred subject to appropriate confidentiality and legal safeguards.

7.4 No sale, ads, or cross-service tracking

We do not sell personal data, share it with data brokers, use it for third-party advertising, or track users across unrelated apps or websites. If this changes, we will update this policy, obtain any required consent, and update the Apple and Google store disclosures before the new processing begins.

8. International transfers and data location

The Service may process data in [HOSTING COUNTRIES/REGIONS] and in countries where the providers above operate. Those countries may have different data protection laws from the user’s country.

Where required, we use an adequacy decision, approved standard contractual clauses, contractual protections, transfer risk assessments, explicit consent, or another lawful transfer mechanism. EU/EEA data transferred to a non-adequate country will use an appropriate Chapter V GDPR mechanism. Saudi, UAE, Chinese, South African, Kenyan, Nigerian, Singaporean, Japanese, Indian, and other local transfer requirements must be evaluated before those countries are enabled.

Mainland China must be treated as a separate launch decision. PIPL notice, separate-consent, local representative, security assessment or standard-contract requirements, localization thresholds, and vendor accessibility must be assessed before offering the Service there.

9. Retention and deletion

We keep personal data only for as long as needed for the purposes above, to provide the user’s requested long-term memory service, and to meet legal, accounting, security, and dispute-resolution requirements.

The following schedule is a **proposed operating commitment and must be confirmed and implemented before publication**:

Data	Proposed retention
Active account/profile	While the account is active
Memories and encrypted files	Until the user deletes them, completes account deletion, or a documented service rule requires deletion

Data	Proposed retention
Recipient records and undelivered assignments	Until the sender deletes them, the recipient objects and deletion is legally required, the related account is deleted, or the purpose expires
Delivered memory links and view state	While either related account/content remains, subject to recipient rights
OTP records	Delete or irreversibly anonymize within 24 hours after expiry or successful use
Revoked/expired refresh tokens	Delete within 30 days after expiry or revocation
Push token	Until logout/removal, invalidation, or account deletion
Server and security logs	30–90 days, extended only for active security or legal matters
Support records	24 months after closure unless a longer legal period applies
Admin audit records	24 months or the documented security/compliance period
Subscription, transaction, tax, and refund records	The legally required accounting/tax period, proposed as 7 years unless local law requires otherwise
Deleted data in backups	Isolated from normal use and overwritten within 90 days, unless preservation is legally required

Deleting a mobile app does not delete the user’s CODA account. The Service must provide an in-app account-deletion request and a public web deletion page before release. When deletion is requested, we will explain any delay, content-delivery consequence, subscription consequence, and legally required retention. Data retained for law or fraud prevention will be isolated and used only for that purpose.

10. User choices and privacy rights

Depending on location, a person may have the right to:

- know whether and how we process their data;
- access or receive a copy of their data;
- correct inaccurate or incomplete data;
- delete data or an account;
- restrict or object to processing;
- withdraw consent without affecting earlier lawful processing;
- receive portable data in a commonly used machine-readable format;
- object to direct marketing;
- complain to a local data protection authority; and
- challenge certain automated decisions.

Requests may be submitted through [\[IN-APP PRIVACY CENTER URL/PATH\]](#), [\[WEB REQUEST URL\]](#), or [\[PRIVACY EMAIL\]](#). We may verify identity and authority before acting. We will respond within the time required by applicable law. Rights may be limited where an exception applies, including another person’s rights, legal obligations, fraud prevention, or legal claims.

Recipients who do not have an account may use the same channels to ask what data CODA holds about them, object to notification, correct their details, or request deletion where applicable.

EU/EEA users may complain to the supervisory authority in their habitual residence, workplace, or place of the alleged infringement. Other users may contact the authority identified in the regional addendum.

11. Notifications and communications

CODA sends communications needed to operate the Service, such as verification codes, security notices, check-in reminders, subscription notices, and memory delivery notices. Device push notifications require operating-system permission and can be disabled in device settings, but disabling reminders may affect a check-in delivery workflow.

Recipient notices are transactional service messages requested by the sender. They must not contain unrelated marketing. Every first recipient notice should identify CODA, identify the source of the recipient data, link to this policy, and provide a simple opt-out/privacy-request method.

We will obtain marketing consent where required before sending promotional email, SMS, or push notifications. [\[CONFIRM: CODA DOES NOT CURRENTLY SEND PROMOTIONAL MESSAGES.\]](#)

12. Children

The proposed Service eligibility age is **18 or older**. CODA is not directed to children, and users must not create an account or provide a child's personal data unless CODA has implemented and documented a legally valid parental/guardian process for the relevant country.

If we learn that a child's data was collected contrary to this rule, we will restrict and delete it as required. Contact [\[PRIVACY EMAIL\]](#) with relevant details. The final age threshold and age-assurance method must be confirmed before publication.

13. Cookies and local device storage

The mobile app stores authentication tokens and limited notification/language state using device-protected or local storage. The website uses strictly necessary authentication/session cookies for login and account management. The current implementation does not use advertising or analytics cookies.

Strictly necessary storage cannot be disabled where it is required to provide a requested login or security function. If analytics, advertising, personalization, or other non-essential cookies/SDKs are added, CODA will first implement a consent-management mechanism where required and update this policy and the store forms.

14. Changes to this policy

We may update this policy to reflect product, legal, security, or provider changes. We will post the updated version, change the "last updated" date, and provide additional notice or seek consent when required. Material changes will not be applied retroactively where prohibited by law.

15. Contact and complaints

Questions and requests may be sent to:

[\[FULL LEGAL ENTITY NAME\]](#)

[\[POSTAL ADDRESS\]](#)

[\[PRIVACY EMAIL\]](#)

[\[SUPPORT URL\]](#)

PART II

Terms of Service

1. Agreement and eligibility

These Terms govern use of the Service. By creating an account or using the Service, the user agrees to these Terms and the Privacy Policy. If the user does not agree, they must not use the Service.

Users must be at least 18 years old, have legal capacity to enter a contract, and use the Service only where it is lawfully offered. A person using CODA for an organization represents that they are authorized to bind it.

2. What CODA provides

CODA provides private storage and user-directed delivery tools for digital memories. Users may prepare content, choose recipients, and select a scheduled or check-in-based delivery rule.

CODA is **not**:

- a will, trust, estate-planning, probate, notary, or legal-document service;
- an emergency, health-monitoring, missing-person, or death-verification service;
- a guaranteed archival or perpetual-storage service; or
- a substitute for independent backups, direct family communication, professional advice, or legally recognized instructions.

A missed check-in does not prove death or incapacity. Users are responsible for maintaining alternative arrangements for legally, financially, or personally critical matters.

3. Accounts and security

Users must provide accurate details, protect passwords and devices, promptly report unauthorized access, and keep recipient information current. Accounts may not be sold, transferred, shared, or used to impersonate another person.

CODA may require verification, temporarily restrict access, revoke sessions, or request additional information when reasonably necessary for security, fraud prevention, or legal compliance.

4. User content and license

Users retain ownership of content they upload. To operate the Service, a user grants CODA a limited, non-exclusive, worldwide license to host, encrypt, store, reproduce, transmit, decrypt, format, and make the content available to the chosen recipient, solely to provide, secure, support, and comply with law in relation to the Service. This license ends when the content is deleted from active systems, subject to backups and legal retention.

The user represents that:

- they own the content or have permission to use and deliver it;
- the content and recipient data do not violate law, privacy, confidentiality, intellectual property, court orders, or another person's rights;
- they have authority or another lawful basis to provide every recipient's contact details; and
- they will not rely on CODA to deliver a legally operative instruction.

Recipients receive only the limited right to access content designated for them through the Service. They may not misuse, redistribute, or commercially exploit it without the owner's or applicable rights holder's permission.

5. Delivery rules

Users select either a scheduled delivery time or an activity check-in rule. Delivery depends on accurate account and recipient details, device/network availability, subscription access, third-party providers, and the Service remaining operational.

Delivery times are targets, not guarantees. Time zones, daylight-saving changes, provider delays, invalid contact details, spam filtering, expired subscriptions, outages, or legal restrictions may delay or prevent notification or access. CODA may pause a delivery reasonably suspected to be erroneous, unlawful, unsafe, or fraudulent.

Users must review their memories, recipient details, schedules, check-in interval, and account access regularly. Sent memories may be locked against editing. Deleting a memory before delivery permanently removes its active content and recipient links.

6. Subscriptions, trials, billing, and refunds

Plan features, quotas, duration, and current price are shown before purchase. Store-displayed localized price and terms control over conflicting promotional text.

- Apple purchases are billed and managed by Apple under the user's Apple account.
- Google Play purchases are billed and managed by Google under the user's Google account.
- Web purchases are billed through Stripe and managed through the CODA web billing portal.
- The basic CODA trial is currently intended to be a one-time, non-renewing 30-day service trial. [\[CONFIRM AGAINST PRODUCTION PLAN CONFIGURATION.\]](#)
- Paid six-month and annual subscriptions automatically renew unless canceled before the renewal date, as disclosed by the applicable billing provider.
- Deleting a CODA account does not necessarily cancel a store subscription. Users must follow the applicable provider's cancellation flow, and CODA must present a direct management link in the app.

Cancellation normally stops future renewal while paid access continues until the end of the current billing period, unless the provider or applicable law requires a different result. Refunds are handled under the billing provider's rules and mandatory local consumer law. Nothing in these Terms limits non-waivable cancellation, refund, cooling-off, conformity, or other consumer rights.

If a subscription expires, access to premium features may be restricted. CODA will not intentionally delete stored memories solely because a plan changes without first giving the notice and options required by the applicable plan terms and law. [\[CONFIRM PRODUCT RULE FOR OVER-QUOTA CONTENT AFTER EXPIRY.\]](#)

7. Acceptable use

Users must comply with the Acceptable Use Policy below. CODA may remove or restrict unlawful content, preserve evidence, suspend delivery, or suspend an account when reasonably necessary to protect people, comply with law, or enforce these Terms. Where appropriate, we will notify the user and provide an appeal route.

8. Intellectual property

CODA and its licensors own the Service, software, design, trademarks, and documentation, excluding user content. These Terms grant a personal, limited, revocable, non-transferable right to use the Service. Users may not copy, resell, reverse engineer, bypass access controls, scrape, probe, or disrupt the Service except where law expressly permits and that right cannot be waived.

9. Account suspension and deletion

Users may stop using the Service at any time and may request account deletion through the in-app and web methods described in the Privacy Policy. Before deletion, users should export any content they are entitled to retain and review subscription cancellation.

Deleting an account may permanently remove undelivered memories and may make delivered content unavailable to recipients. The deletion flow must clearly explain these consequences and require confirmation.

CODA may suspend or terminate an account for material breach, illegal use, security risk, fraud, non-payment, or legal requirement. When reasonable and lawful, CODA will provide notice and an opportunity to cure or appeal. Mandatory consumer and data-protection rights survive termination.

10. Availability and changes

We may maintain, update, modify, or discontinue parts of the Service. For a material reduction to paid functionality, we will provide advance notice and any remedy required by contract or law. Service availability may be affected by maintenance, providers, networks, devices, app stores, force majeure, and events outside our reasonable control.

11. Disclaimers

To the maximum extent allowed by law, the Service is provided “as is” and “as available.” We do not warrant uninterrupted operation, permanent storage, delivery at an exact time, legal effectiveness, or compatibility with every device or file. These exclusions do not apply to warranties or consumer rights that cannot lawfully be excluded.

12. Liability

Nothing in these Terms excludes liability that cannot be excluded, including liability for fraud, willful misconduct, gross negligence where applicable, or death/personal injury caused by negligence where the law prohibits exclusion.

Subject to those rules, CODA is not responsible for indirect or consequential loss, loss caused by inaccurate recipient details, a user’s unlawful content, failure to maintain a check-in, third-party provider outages, or reliance on CODA as a will, emergency service, or sole backup.

Any monetary cap must be approved by local counsel and must preserve mandatory consumer remedies: [\[PROPOSED LIABILITY CAP AND COUNTRY-SPECIFIC EXCEPTIONS\]](#).

13. Governing law and disputes

These Terms are governed by [\[GOVERNING LAW AND COURTS\]](#), except that users retain the protection of mandatory law in their country of residence and any right to bring a claim before a locally competent consumer court or authority.

Do not publish a mandatory arbitration, class-action waiver, or exclusive foreign-court clause without country-specific legal review.

Before filing a claim, users may contact [\[LEGAL/SUPPORT EMAIL\]](#) so the parties can try to resolve the issue informally. This does not shorten a statutory limitation period or restrict access to a regulator or court.

14. Changes to the Terms

We may update these Terms. We will provide reasonable notice of material changes and obtain acceptance when required. Changes do not retroactively reduce accrued rights. If a user rejects a material change, they may stop using the Service and exercise any termination or refund right provided by law.

15. Contact

[\[FULL LEGAL ENTITY NAME\]](#)

[\[POSTAL ADDRESS\]](#)

[\[LEGAL OR SUPPORT EMAIL\]](#)

PART III

Acceptable Use Policy

Users must not use CODA to:

- violate law, sanctions, court orders, or another person's rights;
- upload content they do not own or have permission to process and deliver;
- disclose another person's confidential, intimate, medical, financial, identity, or location data without lawful authority;
- threaten, harass, stalk, coerce, defame, exploit, or facilitate violence or self-harm;
- create or distribute child sexual abuse material, non-consensual intimate content, trafficking content, or sexual exploitation;
- distribute malware, malicious files, credentials, access tokens, or instructions designed to compromise systems;
- impersonate another person, commit fraud, launder money, evade sanctions, or misrepresent a recipient relationship;
- send unsolicited promotional messages or use recipients as a bulk contact or marketing list;
- probe, overload, scrape, reverse engineer, bypass quotas, or interfere with Service security;
- use automation to create abusive accounts, enumerate users, or test stolen credentials; or
- use CODA to make delivery of harmful, illegal, or legally operative instructions appear verified or endorsed by CODA.

CODA may investigate reports, restrict access, block a delivery, preserve relevant evidence, or notify authorities where required. Actions should be proportionate to risk and documented. Users may appeal an enforcement decision at [\[APPEAL EMAIL/URL\]](#).

Report illegal or dangerous content at [\[ABUSE EMAIL/URL\]](#). If someone is in immediate danger, contact local emergency services; CODA is not monitored as an emergency channel.

PART IV

Regional Privacy Addendum

This section supplements the global policy. It is not an exhaustive statement of every law. Launch must be restricted to approved countries until local requirements, registration, representative, transfer, language, consumer, telecom, and data-residency obligations are confirmed.

A. European Union and EEA

- CODA must publish its controller identity, purposes, legal bases, recipients, retention periods, international-transfer safeguards, rights, and complaint route.
- A non-EU controller offering CODA to people in the EU/EEA will generally need a written EU representative unless a narrow exception applies. Given the continuous account service and potentially sensitive private content, CODA should plan to appoint one.
- Complete a Data Protection Impact Assessment before launch because CODA combines long-term private content, third-party recipient data, inactivity signals, and automated post-inactivity delivery.
- Maintain a Record of Processing Activities, processor agreements, subprocessor register, breach procedure, data-rights workflow, and transfer impact assessments.
- Use an adequacy decision or the EU Standard Contractual Clauses plus supplementary measures for relevant transfers outside the EEA.
- Provide recipients with an Article 14-style indirect collection notice no later than the first contact and assess whether earlier notice is required. The current delayed-notification design needs legal review.
- Users may lodge a complaint with their local supervisory authority. Insert the lead authority only after the establishment/representative structure is decided.

B. Asia

Singapore

Confirm consent/notification, purpose limitation, protection, retention, access/correction, breach notification, and comparable protection for overseas transfers. Appoint and publish a Data Protection Officer contact where required.

Japan

Confirm the APPI disclosure, security, breach, individual-rights, and foreign-transfer requirements. Identify foreign recipients and the basis for overseas transfer when required.

India

Track the staged commencement of the Digital Personal Data Protection Act 2023 and Digital Personal Data Protection Rules 2025. Before launch, confirm notice, consent manager/withdrawal, grievance, security, breach, child-data, retention/erasure, and cross-border requirements that are in force on the launch date.

Mainland China

Do not launch solely on the basis of this draft. Complete a PIPL and cybersecurity review covering a China representative, Chinese notice, separate consent for sensitive information and cross-border transfers, data mapping, localization thresholds, standard contract/certification/security assessment, personal information protection impact assessment, government-request controls, and accessible local vendors.

Other Asian countries

Add country-specific terms for every launch market, including relevant rules in South Korea, Indonesia, Malaysia, Thailand, the Philippines, Vietnam, and others. “Asia” is not a single compliance region.

C. Middle East and North Africa

Saudi Arabia

Confirm PDPL lawful basis, Arabic notice, data-subject rights, destruction schedule, DPO/registration obligations, breach handling, and SDAIA transfer requirements. The Saudi PDPL can cover data of deceased persons where it identifies them or their family, which is directly relevant to CODA.

United Arab Emirates

Confirm application of the federal Personal Data Protection Law and whether DIFC or ADGM rules apply to the operator. Validate consent/lawful basis, DPO, breach, rights, and cross-border safeguards.

Bahrain, Qatar, and Egypt

Complete separate reviews for Bahrain Law No. 30 of 2018, Qatar Law No. 13 of 2016, and Egypt Law No. 151 of 2020, including regulator permissions/registrations, sensitive-data rules, direct communications, and overseas transfers.

Other MENA countries

Confirm national privacy, telecom/SMS, e-commerce, cybercrime, consumer, content, and data-hosting requirements before enabling each country.

D. Africa

South Africa

Confirm POPIA responsible-party obligations, register the Information Officer where required, publish PAIA information where applicable, execute operator agreements, handle data-subject rights, assess prior authorization, and validate cross-border transfers and electronic communications.

Nigeria

Confirm obligations under the Nigeria Data Protection Act 2023 and current NDPC guidance, including whether CODA is a data controller/processor of major importance, registration/audit duties, DPO requirements, lawful bases, child data, breach response, and cross-border transfers.

Kenya

Confirm ODPC registration category, Data Protection Act and Regulations compliance, DPIA, processor contracts, rights, breach reporting, and proof of adequate safeguards or consent for transfers outside Kenya.

Other African countries

Review each country separately, including Morocco, Tunisia, Ghana, Rwanda, Uganda, and other intended markets. “Africa” is not a single compliance region.

PART V

Internal Release Requirements

Remove this internal section from the public version after all items are resolved.

Must be completed before store submission

1. Implement authenticated in-app account deletion and a public web deletion-request page. Explain content and subscription consequences, delete associated active data, and preserve only documented legal records.
2. Add working Privacy Policy and Terms links at signup, in Settings/Profile, and on the subscription purchase screen. The current signup labels are not interactive links.
3. Add Apple/Google/Stripe subscription management and cancellation links in the account area.
4. Add recipient indirect-notice content and a privacy/opt-out link at first contact. Decide whether recipients must be notified when entered rather than only when a memory is released.
5. Replace “End-to-End Encrypted & Quantum Secure” everywhere. Current server-side AES-256-GCM encryption does not support that claim.
6. Remove unused permissions or implement and accurately explain the feature. The native projects currently declare microphone, camera, Face ID, and Android recording access although the reviewed user flow selects existing files and plays audio rather than recording it.
7. Add an age confirmation and enforce the approved minimum age/parental process.
8. Build data access/export, correction, recipient objection, and account deletion workflows with auditable response deadlines.
9. Implement and test the approved retention/deletion schedule, including OTP cleanup, logs, backups, object storage, billing exceptions, and pending recipient records.
10. Complete a DPIA, legitimate-interest assessment for recipient processing, transfer impact assessments, vendor DPAs, subprocessor inventory, and incident-response plan.
11. Confirm production HTTPS, infrastructure locations, database backup locations, administrator access controls, key rotation, audit logging, and breach notification contacts.
12. Align the app privacy manifest, App Store privacy labels, Google Data safety form, website policy, and actual code before every release.
13. Provide accurate reviewer credentials and explain scheduled/check-in delivery without requiring reviewers to wait for a real deadline.
14. Translate the final policy and key consent/rights screens for the supported locales using legal-quality review: English, French, Arabic, German, Simplified Chinese, Hindi, Spanish, Portuguese, and Russian.

Clarifications required from the owner

1. What is the full legal company name, registration country/number, registered address, and governing law?
2. Which exact countries will be enabled at launch? Specifically confirm whether mainland China, India, Saudi Arabia, UAE, South Africa, Nigeria, and Kenya are in phase one.
3. Where are the API, MySQL database, logs, backups, and Cloudflare R2 bucket physically hosted?

4. Which email addresses should be public for privacy, support, legal, abuse, and appeals? The code currently references both Info@codaliveforever.com and hello@codaliveforever.com.
5. Is the intended minimum age 18, or will CODA support minors with verified parental/guardian consent?
6. Should a recipient be notified as soon as the sender enters their details, or only when a memory is delivered? Has the recipient consented outside CODA?
7. What should happen to undelivered and already-delivered memories when a sender or recipient deletes their account?
8. What are the approved retention periods for active content, backups, logs, support cases, audit events, OTPs, and billing/tax records?
9. What is the business rule for stored content when a subscription expires or the account exceeds the downgraded quota?
10. Which legal entity is the merchant for Stripe web subscriptions, and are web subscriptions offered inside the mobile app or only on the website?
11. Does CODA plan any analytics, crash reporting, advertising, marketing email/SMS, social login, or third-party SDK not present in the reviewed repositories?
12. Who will act as the EU representative, DPO/privacy lead, South African Information Officer, and any other required local representative?

Official legal references used for the regional framework

- [EU General Data Protection Regulation](#)
- [European Data Protection Board SME guide](#)
- [European Commission international transfer rules](#)
- [Singapore PDPC data protection obligations](#)
- [Japan Personal Information Protection Commission laws and policies](#)
- [India Digital Personal Data Protection Act 2023](#)
- [China Personal Information Protection Law](#)
- [Saudi data protection knowledge center](#)
- [UAE data protection laws](#)
- [South Africa POPIA](#)
- [Nigeria Data Protection Commission](#)
- [Kenya Office of the Data Protection Commissioner](#)