Data Processing Agreement

Last updated: October 26, 2026 (version 1.0)

This agreement forms part of the Ancor Terms of Service. A customer accepts it by using the Ancor service; nothing needs to be signed. If your agency wants a countersigned copy for its records, email hello@getancor.com with your agency's legal name and address and we will send one back signed.

It covers personal data that an agency puts into Ancor. It includes the EU Standard Contractual Clauses and the UK International Data Transfer Addendum for customers in the UK and the EEA, and notes for customers in Australia, New Zealand and the UAE.

1. The parties

Ancor: Rushabh Porwal, a sole proprietor trading as Ancor, GSTIN 27CSNPP8704M1ZW, 102 Rajniketan, Bapubhai Vashi Road, Vile Parle West, Mumbai, Maharashtra 400056, India. Contact: hello@getancor.com.

The Customer: the agency or other organisation that has an Ancor workspace and has agreed to the Terms of Service, as named in its account or in a countersigned copy of this agreement.

Ancor and the Customer are each a "party". This agreement applies for as long as Ancor processes Customer Personal Data.

2. Words used in this agreement

- **Customer Personal Data**: personal data that the Customer or its users put into the service, or that the service creates from it, and that Ancor processes for the Customer. Annex I lists the kinds.

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

Reject non-essential | Accept all | Preferences

Principles; New Zealand's Privacy Act 2020; and the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

- **EU SCCs**: the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021.
- **UK Addendum**: the International Data Transfer Addendum to the EU SCCs, version B1.0, issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, in force from 21 March 2022.
- **Subprocessor**: a company Ancor uses that processes Customer Personal Data.
- **Personal Data Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- "Controller", "processor", "data subject", "processing" and "supervisory authority" have the meanings given in the EU GDPR. Under India's law the Customer is the "data fiduciary" and Ancor the "data processor".

3. Roles

1. For Customer Personal Data, the Customer is the controller and Ancor is the processor (GDPR Article 28). Where the Customer is itself a processor for its own client, Ancor is its subprocessor and the Customer will pass on any instructions from that client.
2. The Customer is responsible for having a lawful basis for the data it puts into Ancor and for telling its staff, contractors and clients about the processing, including the workload and team-health features described in the privacy policy.
3. For data Ancor collects for its own business (the account owner's billing details, its own marketing website analytics, and sales contact with the Customer), Ancor is the controller under its privacy policy, not this agreement.

4. Processing only on the Customer's instructions

1. Ancor processes Customer Personal Data only to provide, secure, support and maintain the

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

3. If a law requires Ancor to process Customer Personal Data in another way, Ancor will tell the Customer before it does so, unless that law forbids telling.
4. Ancor does not sell Customer Personal Data and does not use it for advertising.
5. The Customer instructs Ancor to compute statistics combined across workspaces to give new workspaces sensible starting estimates (for example, how many days a type of deliverable usually takes, used only once at least five agencies contribute). These statistics are numbers, not records: they hold no names or other personal data, and no customer ever sees another customer's projects, clients, people or money.

5. People at Ancor

1. Ancor is one person today: Rushabh Porwal, the founder. As the person who runs the service he has technical access to the production systems, and he uses it only to run, support, secure and fix the service. He is bound by confidentiality.
2. Inside the product, Ancor's admin console can open a Customer's workspace only through a logged access with a written reason and a time limit of at most four hours. The Customer's owners are told in the app and by email each time, can see every access in Settings, and can end it early. Each access, and any change made during it, is recorded in the Customer's audit log.
3. Before anyone else is given access to Customer Personal Data, Ancor will bind them to written confidentiality obligations and give them only the access their work needs.

6. Security

Ancor keeps the technical and organisational measures in Annex II in place (GDPR Article 32). It may change them, but not in a way that lowers the overall protection of Customer Personal Data.

7. Subprocessors

1. The Customer gives Ancor general authorisation to use subprocessors. The current list is in

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

3. The Customer may object on reasonable data protection grounds by emailing hello@getancor.com within that notice period. The parties will try to resolve it in good faith. If they cannot, the Customer may end its subscription before the change takes effect and Ancor will refund any prepaid fees for the unused period.
4. Ancor puts data protection terms in place with each subprocessor that protect Customer Personal Data at least as well as this agreement does, and remains responsible to the Customer for each subprocessor's performance.
5. Tools the Customer chooses to connect to Ancor (for example Slack, Microsoft Teams or Zoho) are the Customer's own providers, not Ancor's subprocessors.

8. Helping the Customer

1. **Data subject requests.** Most requests (access, correction, export, deletion) the Customer can handle itself in the product. Where it cannot, Ancor will help within a reasonable time. If a data subject writes to Ancor directly about Customer Personal Data, Ancor will pass the request to the Customer and will not answer it on the Customer's behalf unless the Customer asks.
2. **Assessments.** Ancor will give the Customer reasonable information it needs for a data protection impact assessment or a consultation with a supervisory authority about the service.

9. Personal data breaches

1. Ancor will notify the Customer without undue delay, and in any case within 48 hours, after becoming aware of a Personal Data Breach.
2. The notice will say, as far as Ancor knows at the time: what happened; the kinds and rough number of people and records affected; the likely consequences; what Ancor has done and will do about it; and who to contact. Ancor will send updates as it learns more, and will take reasonable steps to contain the breach and limit the harm.
3. Notices go to the Customer's workspace owners by email, and to any security contact the

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

10. Return and deletion

1. **Export.** The Customer's owner or an admin can download a full export of the workspace from Settings at any time. If a trial or subscription ends without renewal, the workspace stays read-only for at least 30 days, so the Customer can still sign in and export.
2. **Deletion.** The owner can ask for the workspace to be deleted from Settings or by email. There are 30 days to change one's mind; after that a daily job permanently removes the workspace's records from the production database. Database backups that hold a copy age out within the 30 days each backup is kept.
3. **Uploaded files.** Files uploaded to a workspace are stored separately from the database and are not yet removed by that daily job. Ancor deletes them on request, when the workspace is deleted.
4. Ancor may keep data where a law requires it (for example Ancor's own tax invoices to the Customer), and then only for that purpose.

11. Information and audits

1. Ancor will make available the information needed to show it meets this agreement and GDPR Article 28: this agreement, the security page, the subprocessor list, and written answers to the Customer's reasonable security questions.
2. Ancor does not hold SOC 2, ISO 27001 or other third-party certifications today, and has not had an outside penetration test.
3. If that information is not enough, or a supervisory authority requires it, the Customer may audit Ancor's compliance with this agreement once a year, on at least 30 days' written notice, during business hours in India, at the Customer's own cost, with an auditor bound by confidentiality, and in a way that does not expose other customers' data. The parties will first try a remote review of documents.

12. International transfers

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what’s useful and marketing cookies to measure our ads. How we use cookies

Where the Customer is subject to the EU GDPR for Customer Personal Data and that data is transferred to Ancor, the EU SCCs Module Two (controller to processor) are incorporated into this agreement by reference, with the Customer as data exporter and Ancor as data importer, and completed as follows:

- Clause 7 (docking clause) applies.
- Clause 9(a): Option 2, general written authorisation, with at least 30 days' notice of changes, as in section 7 of this agreement.
- Clause 11(a): the optional independent dispute resolution wording does not apply.
- Clause 13: the competent supervisory authority is as set out in Annex I.C.
- Clause 17: Option 2. The clauses are governed by the law of the EU Member State in which the data exporter is established; where that law does not allow for third-party beneficiary rights, by the law of Ireland.
- Clause 18(b): disputes are resolved by the courts of the EU Member State whose law governs under Clause 17.
- Annex I of the EU SCCs is Annex I of this agreement; Annex II is Annex II; and the list of subprocessors is Annex III.

12.2 Onward transfers to subprocessors: Module 3

Where Ancor, as processor, transfers Customer Personal Data that came under 12.1 or 12.3 to a subprocessor in a country without an adequacy finding, Ancor will do so under the EU SCCs Module Three (processor to processor), with the UK Addendum where UK data is involved, or another transfer mechanism recognised by Data Protection Law, and with terms no less protective than this agreement.

12.3 Customers in the UK: the UK Addendum

Where the Customer is subject to the UK GDPR, the UK Addendum is incorporated into this agreement by reference and applies to transfers of Customer Personal Data to Ancor, completed as follows:

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

- Table 3 (appendix information): Annexes I, II and III of this agreement.
- Table 4 (ending this Addendum when the Approved Addendum changes): either party may end it as allowed by Section 19 of the UK Addendum.
- Part 2 (Mandatory Clauses): the Mandatory Clauses of the Approved Addendum, template B1.0, issued by the Information Commissioner and laid before Parliament under section 119A of the Data Protection Act 2018 on 2 February 2022, as revised under its Section 18.

12.4 Customers in Switzerland

Where the Swiss Federal Act on Data Protection applies, the EU SCCs under 12.1 apply with these changes: the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for transfers under Swiss law; references to "Member State" include Switzerland so that data subjects in Switzerland can sue there; and references to the GDPR include the Swiss Act.

12.5 Order of precedence

If the EU SCCs or the UK Addendum conflict with the rest of this agreement, the EU SCCs or the UK Addendum win.

13. Customers in Australia and New Zealand

1. Where the Customer is subject to Australia's Privacy Act 1988 (Cth), Ancor will handle Customer Personal Data in a way consistent with the Australian Privacy Principles that would apply to the Customer, including APP 11 (security). The Customer is told by this agreement and the subprocessors page that the data is held in India and the other countries listed in Annex III, which it can rely on for APP 8 (cross-border disclosure) and for its own privacy notice.
2. Ancor's breach notice under section 9 is meant to let the Customer assess whether a breach is an eligible data breach under the Notifiable Data Breaches scheme and notify the Office of the Australian Information Commissioner and affected people where it must.

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

14. Customers in the UAE

1. Where the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data applies, the Customer is the controller and Ancor the processor under that law. Ancor's commitments in sections 4 to 11 apply to that data.
2. The data is transferred to India and the other countries in Annex III. The Customer is responsible for having a basis for that transfer under Articles 22 and 23 of the Decree-Law, and Ancor will sign further reasonable transfer terms if the Customer needs them.
3. Customers in a free zone with its own data protection law, such as the DIFC or ADGM, can ask for the transfer terms that law requires, and Ancor will work with them in good faith.

15. India

Under India's Digital Personal Data Protection Act, 2023, the Customer is the data fiduciary and Ancor processes Customer Personal Data on its behalf under this agreement. Sections 4 to 11 apply.

16. General

1. This agreement lasts as long as Ancor processes Customer Personal Data. Sections 9, 10 and 11 survive until that data is deleted.
2. Each party's liability under this agreement is subject to the limits in the Terms of Service, except where Data Protection Law or the EU SCCs do not allow liability to be limited.
3. If this agreement and the Terms of Service conflict about personal data, this agreement wins, subject to section 12.5.
4. Except for the EU SCCs and the UK Addendum, which are governed as they say, this agreement is governed by the same law and courts as the Terms of Service.
5. Ancor may update this agreement by posting a new version on this page. It will give at least 30 days' notice by email of a change that reduces the protection of Customer Personal Data, and will not reduce it below what Data Protection Law requires.

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

Data exporter (controller)	The Customer, as named in its Ancor account. Contact: the workspace owner. Activities: running an agency and using Ancor to manage projects, people, time, clients and invoicing. Signature: acceptance of the Terms of Service, or a countersigned copy.
Data importer (processor)	Rushabh Porwal, trading as Ancor, 102 Rajniketan, Bapubhai Vashi Road, Vile Parle West, Mumbai, Maharashtra 400056, India. Contact: Rushabh Porwal, proprietor, hello@getancor.com. Activities: providing the Ancor agency management service. Signature: by publishing this agreement, or a countersigned copy.

B. The transfer and the processing

Data subjects	The Customer's owners, admins, staff and contractors who use Ancor; the Customer's clients and their contacts who use the client portal or are named in the workspace; other people named in content the Customer puts into Ancor.
Personal data	Names, work email addresses, job titles, roles, departments, skills, profile photos and reporting lines; timesheets, work logs, task assignments and task timing; sign-in records, session times, IP addresses and device or browser details; audit log entries; pay figures if the Customer enters them; client contact names and email addresses; comments, approvals and uploaded files; invoice details of the Customer's clients (names, addresses, tax numbers); text extracted from a resume if a user uploads one (the file itself is not stored).
Sensitive data	Optional self-reported mood and energy check-ins, and wellbeing indicators computed from work patterns, which could reveal something about a person's health. Safeguards: they are visible only to the workspace's owners and admins, the Customer decides whether its team uses them, and the measures in Annex II apply. Ancor does not ask for any other special category data.
Frequency	Continuous, for as long as the Customer uses the service.
Nature of the processing	Hosting, storage, computation and display in the app and client portal; AI features (planning, reports, skill extraction); sending email; backups; support; deletion.
Purpose	To provide, secure, support and maintain the Ancor service for the Customer.

Cookies, plainly.

Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

Transfers to subprocessors	As in Annex III, for the purposes and for the time stated there.

C. Competent supervisory authority

Under the EU SCCs, Clause 13: the supervisory authority of the EU Member State where the Customer is established. If the Customer is not established in the EU but falls under the EU GDPR through Article 3(2) and has appointed a representative, the authority of the Member State where that representative is established; if it has no representative, the authority of the Member State where the data subjects whose data is transferred are located. For the UK Addendum: the UK Information Commissioner's Office. For Switzerland: the Federal Data Protection and Information Commissioner.

Annex II. Technical and organisational measures

As of the date at the top of this page.

Where data is held	The application (Google Cloud Run), database (Supabase PostgreSQL), AI (Gemini on Google Vertex AI), uploaded files and daily backups (Google Cloud Storage) are in Mumbai, India. Other providers and their locations are in Annex III.
Encryption in transit	HTTPS (TLS) on every connection, with HSTS on getancor.com; TLS from the application to the database and to the cache.
Encryption at rest	The database, backups and stored files are on disks the providers encrypt. On top of that, Ancor encrypts pay figures, the access and refresh tokens of connected tools, and two-factor secrets with AES-256-GCM before storing them.
Sign-in	Passwords stored only as Argon2 hashes; temporary lock after repeated failed sign-ins; optional two-factor sign-in for every user (authenticator app, with one-time backup codes); rate limits on sign-in and other endpoints; CSRF protection. The founder's Ancor admin account uses two-factor sign-in, and the Google Cloud account that runs Ancor has 2-step verification on.
Access	Role-based permissions. Members see pay, revenue, billing rates and invoices only if their role allows it.

Cookies, plainly.
Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies

Separation between customers	Every request is tied to the workspace the person signed in to, and data is read and written only for that workspace. Automated tests guard the money queries.
Access by Ancor	Opening a customer's workspace from Ancor's admin console needs a logged access with a written reason and a time limit of at most four hours; owners are told in the app and by email and can see and end each access in Settings; each access, and any change made during it, is recorded in the workspace's audit log. As the operator, the founder also has technical access to the production systems.
Audit logging	Sign-ins, failed sign-ins, data exports, deletion requests, role changes, two-factor changes, access to pay figures and other sensitive actions are recorded with who did it and when. Kept for 2 years.
Secrets	Database passwords and API keys are held in Google Secret Manager, not in the code.
AI	Gemini models on Vertex AI in Mumbai. Under Google Cloud's terms for Vertex AI, Google does not use this data to train its models. Before a prompt is sent, the server strips values that look like secrets (API keys, access tokens, private keys) and trims oversized text.
Backups and recovery	A full database backup once a day, each kept 30 days, in Mumbai. A restore was tested on 23 October 2026: the newest backup restored into a fresh database without errors.
Monitoring	Uptime checks on the API every 5 minutes and an error-rate alert, both emailing the founder; application errors reported to Sentry with passwords, tokens and cookies removed.
Export and deletion	Self-serve full export from Settings; workspace deletion after a 30-day window by a daily job, as in section 10.
Not in place	No SOC 2 or ISO 27001 certificate and no third-party penetration test; a single region with no standby; daily backups without point-in-time recovery (up to a day of entries could be lost), held in the same Google Cloud account as the app; owners cannot yet require two-factor sign-in for their whole team; no 24-hour on-call team.

Cookies, plainly.

Essential cookies keep the site working. With your OK, we also use analytics to see what’s useful and marketing cookies to measure our ads. How we use cookies

PROVIDER	WHAT IT DOES	WHERE
Google Cloud (Cloud Run, Cloud Storage, Secret Manager, Cloud Logging)	Runs the application, stores uploaded files and backups, holds secrets, keeps server logs	Mumbai, India. Server logs are kept in Google Cloud Logging's global storage.
Google Vertex AI	Runs the AI features on Gemini models	Mumbai, India
Supabase	Hosts the PostgreSQL database	Mumbai, India (AWS ap-south-1)
Upstash	Redis: rate-limit counters, and short-lived copies (30 minutes at most) of sign-in session data and some computed summaries	Tokyo, Japan (Google Cloud)
Resend	Sends the service's email: invites, notifications, invoices sent by email	Sends from Tokyo, Japan (AWS); Resend is a US company
Sentry	Error monitoring; an error report can include the user's ID, email address, workspace ID and request details	United States
PostHog	In-app product analytics, only after the user agrees to analytics cookies; typed inputs are masked	European Union
Firebase Hosting (Google)	Serves the website and app files and forwards app requests to the application	Global edge network
Cloudflare	DNS and network in front of getancor.com; all traffic passes through it encrypted	Global edge network
Razorpay	Takes payment for the Customer's Ancor subscription	India

Cookies, plainly.

Essential cookies keep the site working. With your OK, we also use analytics to see what’s useful and marketing cookies to measure our ads. How we use cookies

	CUSTOMER (CONTROLLER)	ANCOR (PROCESSOR)
Legal name		Rushabh Porwal, trading as Ancor
Address		102 Rajniketan, Bapubhai Vashi Road, Vile Parle West, Mumbai 400056, India
Signed by		Rushabh Porwal
Title		Proprietor
Signature		
Date		

Cookies, plainly.

Essential cookies keep the site working. With your OK, we also use analytics to see what's useful and marketing cookies to measure our ads. How we use cookies