Data Processing Agreement — Common Paper DPA v1.1 Cover Page + security schedule stub

DRAFT — not reviewed by counsel. NOT EXECUTED. NOT LEGAL ADVICE. COMPANY-LEDGER C3; D261 (2026-10-14) paper lane; research `~/tb-artifacts/reserve-ledger/records/gate-review-20261014/research-R3.json` item "C3 data processing agreement + security schedule" (recommendation `common_paper_dpa_v1_1`, confidence high).

Trigger that turns this draft into a signature: the first design partner whose statements carry counterparty personal data (holding custodian statements makes ReserveBeat a processor of counterparty PII — the C3 row). It attaches to the C2 Design Partner Agreement or, later, to the C4 Cloud Service Agreement. Signature is Aaron's act as Sole Member.

Version check (fetched 2026-10-14): `https://commonpaper.com/standards/data-processing-agreement/` reads "Current version: 1.1"; its Cover Page incorporates "the Common Paper DPA Standard Terms Version 1.1 posted at commonpaper.com/standards/data-processing-agreement/1.1/". The page states the DPA supports Controller-to-Processor and Processor-to-Subprocessor relationships, that the Cover Page "contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs" and "the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum", that the CCPA service-provider row is optional, and that the agreement is "free to use and modify under CC BY 4.0 … as long as you leave in the attribution". The 72-hour breach-notice and 10-business-day subprocessor notice defaults are taken from research-R3 (retrieved 2026-10-13), not re-read today; confirm against the posted 1.1 text at signature.

Attribution (CC BY 4.0, keep on the signed copy): This Cover Page incorporates the Common Paper DPA Standard Terms Version 1.1 (https://commonpaper.com/standards/data-processing-agreement/1.1/), by Common Paper, used under the Creative Commons Attribution 4.0 International licence (https://creativecommons.org/licenses/by/4.0/). Changes from the published form: variables, subprocessor list and security measures filled for ReserveBeat LLC; the Standard Terms are not modified.

COVER PAGE — Data Processing Agreement

This DPA has two parts: (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1.1 posted at commonpaper.com/standards/data-processing-agreement/1.1/ ("DPA Standard Terms"), which are incorporated by reference. If there is any inconsistency, this Cover Page controls.

Parties and roles

	Customer (Data Exporter)	**Provider (Data Importer)**
Legal name	[PARTNER LEGAL NAME]	**ReserveBeat LLC**, a North Carolina limited liability company
Role	[x] Controller [ ] Processor	Processor (or Subprocessor when Customer is a Processor)
Contact	[PARTNER NOTICE EMAIL]	contact@reservebeat.com; postal line: see https://reservebeat.com/contact
Signatory	[NAME, TITLE]	Aaron Cohen, Sole Member

Key Terms

Variable	Value
Agreement	The Design Partner Agreement (`docs/legal/drafts/C2-design-partner-common-paper-v1.3.md`) or Cloud Service Agreement (`C4-csa-common-paper-v2.1-order-form.md`) between the parties, dated [DATE].
Effective Date	Date of last Cover Page signature
Subject matter and purpose of Processing	Provider's review of statements the Customer supplies (custodian, fund and bank statements, and their supporting schedules) to prepare reserve figures, reconciliations and evidence bundles for the Customer, and to operate the hosted service for the Customer's users.
Nature of Processing	Receipt, parsing, tokenisation, reconciliation, storage, hash-chaining and deletion. Provider does not sell Personal Data and does not use it to train models.
Duration	The term of the Agreement plus the deletion period in the Security Schedule.
Categories of Data Subjects	The Customer's counterparties (payers, payees, account holders named in statements); the Customer's staff who hold accounts on the service.
Categories of Personal Data	Counterparty names and account identifiers as they appear in statements (stored only as HMAC tokens after ingestion — Security Schedule §1); business contact details of Customer staff (name, work email, role). No special-category data is intended; Customer agrees not to supply it.
Frequency of transfer	Continuous during the Agreement (statement drops monthly or as agreed).
Approved Subprocessors	See the table below.
Subprocessor notice	Provider gives [10] business days' notice of a new Subprocessor by email to the Customer contact above (DPA Standard Terms default per research-R3; confirm).
Security Incident notice	Without undue delay and in any case within [72] hours of Provider becoming aware (default per research-R3; confirm).
Deletion / return	On termination, Customer data is returned on request and deleted within [30] days, except evidence artifacts retained under the Security Schedule §3 and audit records that are append-only by design.
CCPA service-provider row	[ ] Included (only if Customer has California data subjects) [x] Deleted
Governing Law of the DPA	As the Agreement (North Carolina), except where the SCCs or UK Addendum require an EU member state or UK law.

Approved Subprocessors (Annex III)

Subprocessor	Service	Location	What it sees	Source
DigitalOcean, LLC	Hosting (the droplet that runs the service and its database)	United States	Everything stored at rest	`packages/strings/claims.json privacy_processors_hosting`; `/privacy`
PostHog, Inc.	Product analytics	United States	Named product events; session recordings only from a browser that opted in; cookies stripped	`claims.json privacy_processors_analytics`

Subprocessor	Service	Location	What it sees	Source
Stripe, Inc.	Payments (once compute-unit purchases are switched on)	United States	Account email, units bought, campaign parameters; card data goes to Stripe only	`claims.json privacy_processors_payments`
Resend (email relay)	Transactional email (confirmations, alerts)	United States	The recipient address in the envelope only	COMPANY-LEDGER C3 names Resend; `claims.json privacy_processors_email`
Google LLC	Sign in with Google (optional, when lit)	United States	Email, verified flag and account id for users who choose it	`claims.json privacy_processors_google`

Not Subprocessors (no Customer Personal Data crosses them): blockchains and RPC providers, issuers' published reports, timestamping services (RFC 3161 / OpenTimestamps), content and link tooling (`claims.json privacy_processors_scope`).

Standard Contractual Clauses and UK Addendum

Transfer situation	Instrument	Module
Customer in the EEA, Provider in the US	EU SCCs, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (bundled by the DPA Standard Terms)	Module Two (controller to processor) or Module Three (processor to processor), per the Customer's role above
Customer in the UK	UK International Data Transfer Addendum to the EU SCCs (ICO; in force 21 March 2022), bundled by the DPA Standard Terms	Same module, with the Addendum's Tables filled from this Cover Page
Customer in the US	No transfer module applies; the DPA Standard Terms alone govern	—

Annex I is the Parties / Key Terms tables above; Annex II is the Security Schedule below; Annex III is the Subprocessor table. Competent supervisory authority, if a transfer module applies: [Customer's member-state authority].

SECURITY SCHEDULE (Annex II) — stub, transcribed from the repo's own documents

Every line below cites where the fact lives. Nothing here claims a report or a certification: **ReserveBeat has no SOC 2 report** (`docs/SOC2_HYGIENE.md`, first paragraph). Items marked UNKNOWN are not yet stated anywhere in the repo and are Aaron's to confirm before signature.

#	Measure	What is in place	Evidence
1	Pseudonymisation of counterparty data	Bank-file counterparty identifiers are HMAC-tokenised with an environment-bound key; ingestion fails closed when the key is missing	`docs/SOC2_HYGIENE.md` "Confidentiality — PII (D38)"; key cost in `docs/RUNBOOK-KEY-ROTATION.md` §5.1
2	Raw-file retention	Raw bank files age out at 90 days	`docs/SOC2_HYGIENE.md` "PII (D38)"

#	Measure	What is in place	Evidence
3	Evidence retention	Evidence artifacts kept 7 years (`retention_years`); restatement by supersession, never by edit	`docs/SOC2_HYGIENE.md` "Availability & recovery — Retention"; "Evidence integrity"
4	Access control	Server-side credential check in one place, scrypt hashes; 12-hour HS256 JWTs signed by an env-bound secret that fails closed; `RESERVE_AUTH_REQUIRED=1` walls every route except `/healthz` and `/auth/login`	`docs/SOC2_HYGIENE.md` "Access control — Authentication"
5	Authorisation and least privilege	Roles in an append-only `user_role_history`; auditor tokens rejected on non-read methods; API runs as a SELECT-only role with row-level security pinned to the tenant	`docs/SOC2_HYGIENE.md` "Authorization", "Least privilege in the database (D11)"
6	Audit trail	`audit_log` rows for logins (incl. failures), role changes, ingestion, reconciliation, break and bundle lifecycle; maker/checker enforced in code	`docs/SOC2_HYGIENE.md` "Change management & auditability"
7	Integrity of evidence	Hash-chained artifacts, externally anchored (RFC 3161 + OpenTimestamps) nightly; offline mode discloses itself	`docs/SOC2_HYGIENE.md`; `docs/board/METHODOLOGY.md` §5
8	Secrets handling	Secrets only in environment variables; `deploy/.env.prod` mode 0600, gitignored; rotation annually or on exposure, per-key procedure	`docs/SOC2_HYGIENE.md` "Secrets (F27)"; `docs/RUNBOOK-KEY-ROTATION.md`
9	Backups and recovery	Nightly `pg_dump`; off-droplet pull; restore drilled (2026-07-19 PASSED; 2026-10-05 RTO 228 s); dead-man pages a human when a dump is stale	`docs/RUNBOOK-backup-restore.md`; `docs/DRILLS.md` Drill 4 and Drill 7
10	Incident response	Severity table, detect / contain / preserve-evidence / notify / post-mortem procedure	`docs/RUNBOOK-INCIDENT-RESPONSE.md`
11	Secure development	SAST gate (semgrep, ruff, eslint, actionlint) and DAST gate (ZAP against a throwaway stack) in CI; gitleaks in CI; dependency review monthly	`docs/SAST.md`; `docs/DAST.md`; `docs/SOC2_HYGIENE.md` gaps table; `docs/CONSOLE-BATCH.md` §16
12	Transport encryption	TLS terminated at the Caddy edge for reservebeat.com; HSTS, nosniff, referrer-policy and frame-options measured on prod (2026-10-12/14)	`docs/CONSOLE-BATCH.md` §14.2 row 1
13	Vulnerability disclosure	`/security` page and `security.txt`; disclose.io core safe-harbor terms adopted; acknowledgement target five business days (not a service level)	`packages/strings/claims.json` `security_txt_note`, `security_*`
14	Known gaps, stated	No MFA/SSO (named trigger in `docs/QUESTIONS-HELD.md` §5.1); no off-host log shipping; single host, no failover; backups copied off-host but same-region	`docs/SOC2_HYGIENE.md` "Known gaps"
15	Personnel	One operator (the Sole Member); no staff, no contractors with data access	COMPANY-LEDGER E1/E7; headcount is a fact of the entity, not a control
16	Device / endpoint controls on the operator's machines	**UNKNOWN — ask Aaron** (disk encryption, screen lock, OS patch cadence are not recorded in the repo)	—

#	Measure	What is in place	Evidence
17	MFA on vendor consoles (DigitalOcean, GitHub, registrar, Alchemy, Stripe)	**UNKNOWN — ask Aaron** (GitHub 2FA is implied by `docs/CONSOLE-BATCH.md` §4 but the others are not recorded)	—
18	Insurance	None bound; I1–I4 are DEFERRED, traction-gated (D222). A COI request from a partner is itself a D222 re-open trigger.	`docs/legal/COMPANY-LEDGER.md` I1–I4; DECISIONS D222

Signatures

[PARTNER LEGAL NAME] (Customer)	**ReserveBeat LLC (Provider)**
By: _____	By: _____
Name:	Name: Aaron Cohen
Title:	Title: Sole Member
Date:	Date: _____

Sources

- research-R3.json item "C3 data processing agreement + security schedule" — options (Common Paper DPA v1.1 vs Bonterms DPA vs Art. 28 SCCs alone), field check (Dune publishes a DPA; Messari holds SOC 2 Type II), sources retrieved 2026-10-13: https://commonpaper.com/standards/data-processing-agreement/ ; https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (Decision 2021/914, 4 June 2021); https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj (Art. 28(7) clauses); https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-standard-data-protection-clauses-the-uk-idta-and-the-addendum/ (IDTA and Addendum in force 21 March 2022).
- https://commonpaper.com/standards/data-processing-agreement/ — "Current version: 1.1"; annex mapping; CCPA row optional; CC BY 4.0. Retrieved 2026-10-14.
- `docs/SOC2_HYGIENE.md`, `docs/RUNBOOK-KEY-ROTATION.md`, `docs/RUNBOOK-backup-restore.md`, `docs/DRILLS.md`, `docs/RUNBOOK-INCIDENT-RESPONSE.md`, `docs/SAST.md`, `docs/DAST.md`, `docs/board/METHODOLOGY.md` §5, `packages/strings/claims.json` (`privacy_processors_*`, `security_*`) — the facts in the Security Schedule.