Data Processing Agreement (DPA)

Version: 2026-04 · **Owner:** Legal + Engineering · **Distributed as:** `Votriz_Data_Processing_Agreement.pdf`

This DPA is the standard set of contractual clauses covering data protection, sub-processor handling, and breach notification. It forms part of the customer's master service agreement; nothing here overrides clauses negotiated in an Enterprise contract.

1. Roles

- **Customer** — controller of personal data ingested into Votriz (email subscribers, content authors, social account holders).
- **Votriz / Fortunato AI Inc.** — processor of that personal data on the Customer's behalf.

2. Scope of processing

Votriz processes personal data only for the purposes documented in the master service agreement: AI-assisted content generation, multi-channel publishing, email marketing, brand monitoring, SEO analysis, audience analytics. No personal data is processed for profile-building, advertising attribution, or sale to third parties.

3. Sub-processors

Votriz uses the following sub-processors. Customer is notified of material changes (additions or removals) at least 30 days before they take effect, with the right to object via security@votriz.com.

Sub-processor	Purpose	Data category	Region
Anthropic, PBC	LLM inference (Claude Haiku)	Content prompts, brand voice excerpts	US
OpenAI, LLC	LLM fallback	Same shape as Anthropic payloads	US
fal.ai	Image generation	Text prompts only	US
Resend.com	Transactional + campaign email delivery	Recipient address, email body	US / EU
Stripe, Inc.	Subscription billing	Customer email, billing details	US / EU
Cloudflare, Inc.	TLS termination, CDN, DNS	Public-facing traffic metadata	Global edge
DigitalOcean / Linode (region varies per deployment)	Hosting	All processed data	Customer-selectable on Enterprise

The full sub-processor list with current addresses lives in `votriz-web/public/docs/Votriz_Data_Processing_Agreement.pdf`.

4. Data categories

Category	Examples	Stored where
Account	Email, name, role	`users`, `orgs`
Brand	Brand name, industry, voice profile	`brands`, `brand_memory`
Channel	OAuth tokens (encrypted), platform handle, follower count	`channels`
Content	Drafted posts, approval state, edits	`content_queue`, `published_posts`
Subscriber	Email, name, tags, lead score	`email_subscribers`
Engagement	Opens, clicks, replies, mentions	`email_sends`, `mentions`
Audit	Every authenticated action	`security_audit_log`, `audit_log`

5. International transfers

Data may be transferred to the US via the sub-processors listed above. For EU customers, transfers rely on the EU-US Data Privacy Framework (where the sub-processor is certified) and Standard Contractual Clauses where it isn't. EU-resident processing is available as an Enterprise option.

6. Security measures

The full technical detail lives in `SECURITY_ARCHITECTURE.md`. Headline controls:

- AES-256 at rest (OAuth tokens via Fernet; database at the disk layer); TLS 1.3 in transit.
- Five-role RBAC with brand-level scoping; immutable audit log with database-trigger-enforced append-only semantics.
- Three-layer multi-tenant isolation (application, RLS, optional dedicated infra) verified by the `pre_prod_validation.sh` pre-deploy gate.
- 7-year audit log retention.

7. Breach notification

If Votriz becomes aware of a personal-data breach, Customer is notified without undue delay and in any case within **72 hours** of becoming aware, in accordance with GDPR Article 33. Notification includes:

- Nature of the breach + categories of data affected
- Estimated number of data subjects + records
- Likely consequences
- Measures Votriz has taken or proposes to take

The internal trigger for the 72-hour clock is documented in `AI_INCIDENT_RESPONSE.md` §1 (Severity P1).

8. Data subject rights

Customer is responsible for upstream consent and for honoring data subject rights toward end users. Votriz provides the following endpoints to support that:

Right	How
Access (Art 15)	`GET /settings/export-data` returns all org-scoped data as JSON
Rectification (Art 16)	Standard PATCH endpoints on subscribers, brands, etc.
Erasure (Art 17)	`POST /auth/deletion-request` queues a vetted deletion; `DELETE /email/subscribers/{id}` for per-row removal
Portability (Art 20)	Same as access — the JSON export is the portable format
Object (Art 21)	Email opt-out via `unsubscribe_url` in every campaign; status flips to `unsubscribed` immediately

9. Retention

See `DATA_RETENTION_POLICY.md` for the full retention schedule. Headline: account data is held for the life of the subscription plus 30 days after cancellation; audit logs are retained for 7 years; AI prompts are ephemeral and not stored beyond the inference call.

10. Termination

On termination of the master agreement, Votriz will, at the Customer's choice:

- Return all personal data via `/settings/export-data` (JSON)
- Delete all personal data within 30 days

Audit log entries are retained for the full 7-year period after deletion of the rest of the data, as required by SOC 2 evidence collection.

11. Liability and amendments

Liability terms are governed by the master service agreement. Material amendments to this DPA require notice to Customer at least 30 days in advance.

Contact

- Privacy + DPA questions: privacy@votriz.com
- Security incidents: security@votriz.com
- Legal: legal@fortunatoai.com