Mabble Helix - Sub-Processor / Vendor Risk Matrix

This matrix is the canonical Mabble sub-processor inventory with risk-tier assessment. It is the supporting evidence behind:

- BAA §5 sub-processor disclosure obligation;
- DPA Art. 28(2) general written authorisation;
- CCPA / CPRA Service-Provider chain-of-control attestation;
- SOC 2 (future) sub-service organisation listing;
- Customer Vendor Risk Management questionnaires (CAIQ STA-01, SIG-Lite O.1).

The matrix is generated by hand today and is targeted to be machine-generated from the Phase 4 `vendor_snapshots` table (R-P4.1) after launch, so that the diff-alert system (R-P4.2) keeps it current.

1. Risk tiering

Each vendor is assigned a risk tier based on the data categories the vendor receives and the role the vendor plays.

Tier	Definition	Examples
T1 - Critical	The vendor receives or stores customer-uploaded PHI / personal data, OR holds key material that protects customer data. Loss of the vendor would directly compromise customer data.	AWS (RDS / S3 / KMS), AWS CloudHSM (where opted in by a BYOK customer)
T2 - High	The vendor processes operational metadata that, in aggregate, could allow re-identification or sensitive inference, OR provides controls that protect the audit chain.	Sigstore Rekor (audit anchor), AWS CloudWatch / GuardDuty
T3 - Medium	The vendor processes pseudonymised operational telemetry or non-PHI account / billing data.	Stripe (if billing is enabled in the future)
T4 - Low	The vendor receives only non-customer-identifying operational data (build artefacts, generic email).	GitHub, Atlassian Statuspage (if enabled)
N/A	Listed for transparency but does not currently receive customer data.	Datadog (operational telemetry; planned, not in production)

Onboarding criteria for a T1 / T2 vendor:

1. Signed BAA (where the vendor will receive PHI) or DPA (where the vendor will receive personal data of EU data subjects).
2. SOC 2 Type II report or equivalent (ISO 27001, HITRUST) on file.

3. Documented breach reporting commitment <= Helix's outbound BAA timing (30 days).
4. Audit-right clause (max 1x per year, reasonable notice).
5. Sub-sub-processor disclosure on request.

Vendors not meeting all five may not be onboarded as T1 / T2.

2. Matrix

Vendor	Service	Data categories processed	Residency	BAA	DPA	SOC 2	Sub-contracted to	Risk tier	Last reviewed	Diff-alert subscribed
AWS (Amazon Web Services) - RDS for PostgreSQL	Primary database hosting the encrypted vault store	All customer-uploaded data (encrypted at rest with AES-256-GCM application-layer encryption before AWS sees it)	us-east-1 (default) / eu-west-1 (EU customers)	Yes - AWS BAA executed	Yes - AWS GDPR DPA in effect	Yes - Type II annually	Listed in AWS's published sub-processor list	T1 - Critical	2026-05-14	Yes
AWS - S3	Encrypted backup snapshots, audit-log archive (Object Lock COMPLIANCE 7-year)	All customer-uploaded data (encrypted) plus audit log entries	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T1 - Critical	2026-05-14	Yes

AWS - KMS	Root key custody (CMKs); per-tenant DEK envelope-wrap	Cryptographic key material; no customer payload data	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually. FIPS 140-3 validated HSM-backed	AWS sub-processors	T1 - Critical	2026-05-14	Yes
AWS - CloudHSM	FIPS 140-3 Level 3 HSM for BYOK customers (opt-in)	Cryptographic key material only	Per customer's selected region	Yes - AWS BAA	Yes	Yes - Type II annually; FIPS 140-3 L3 validated	AWS sub-processors	T1 - Critical	2026-05-14	Yes
AWS - Secrets Manager	Application secret storage (DB credentials, API keys, etc.) accessed via External Secrets Operator	Non-customer-identifying operational secrets	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T2 - High	2026-05-14	Yes
AWS - ElastiCache (Valkey 8.2)	Application cache for session and permission lookups (no PHI persisted; entries TTL'd)	Session tokens, RBAC lookup keys; no PHI bodies	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T2 - High	2026-05-14	Yes

AWS - Route 53	Authoritative DNS for customer-facing domains	DNS query metadata only	Global edge	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T3 - Medium	2026-05-14	Yes
AWS - CloudFront + WAF + Shield Standard	Customer-facing CDN, web-application firewall, layer-3/4 DDoS protection	Request metadata (IP, user agent, path); body proxied to origin under TLS 1.3	Global edge	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T2 - High	2026-05-14	Yes
AWS - CloudWatch + GuardDuty	Operational logs, metrics, threat detection	Operational telemetry; PII scrubbed at log boundary by Helix code	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T2 - High	2026-05-14	Yes
AWS - EKS (Kubernetes control plane)	Container orchestration	Operational metadata only	us-east-1 / eu-west-1	Yes - AWS BAA	Yes	Yes - Type II annually	AWS sub-processors	T2 - High	2026-05-14	Yes

Sigstore Rekor	External transparency-log anchor for the audit-log Merkle chain (D-005); Ed25519 signed Merkle tree heads anchored daily	Cryptographic hashes only - no customer data leaves Helix; only the root hash of the audit Merkle tree	Public US infrastructure (Sigstore is hosted by the Linux Foundation)	N/A - no PHI transmitted	N/A - no personal data transmitted	N/A - public-good infrastructure; SOC 2-equivalent operational practice	Linux Foundation sub-infrastructure providers	T2 - High (integrity)	2026-05-14	Yes
GitHub	Source code hosting; CI / CD via GitHub Actions; container image registry	Helix source code; no customer data	US	N/A - Helix source code only	Yes - GitHub DPA	Yes - Type II annually (Microsoft)	Microsoft sub-processors	T4 - Low	2026-05-14	Yes
Cloudflare (planned, not yet in production)	Email-DNS records and external monitoring	DNS query metadata; no PHI	Global edge	Will require BAA when in production	Will require DPA	Yes - Type II annually	Cloudflare sub-processors	N/A - not currently used	2026-05-14	n/a
Datadog (planned, not yet in production)	Operational APM and tracing	Operational telemetry only; PII scrubbed at telemetry boundary	US (multi-region)	Will require BAA when in production	Will require DPA	Yes - Type II annually	Datadog sub-processors	N/A - not currently used	2026-05-14	n/a

Postmark / Amazon SES (transactional email - operating provider selected per environment)	Transactional email for sign-up, password-reset, DSAR fulfilment notice, etc.	Email address + minimal templated body content. Body content is non-PHI by design; PHI is never sent in transactional email.	US	Yes (when SES used - covered by AWS BAA); N/A for Postmark today (Postmark is not currently the production sender)	Yes (SES); Postmark DPA on file if/when activated	Yes (SES - AWS Type II); Postmark Type II annually	AWS / Postmark sub-processors	T3 - Medium	2026-05-14	Yes (SES)
Stripe (planned for billing only - not currently in production)	Subscription billing (when activated)	Billing identifiers, payment-method metadata held by Stripe (Helix is out of PCI scope)	US	N/A - no PHI; billing data only	Yes - Stripe DPA when activated	Yes - Type II + PCI-DSS Level 1 attestation	Stripe sub-processors	T3 - Medium	2026-05-14	n/a - not currently used
DocuSign (planned for BAA / DPA execution)	E-signature of legal documents	Signer name, email, signing metadata; minimal contract body content (legal-document text, not PHI)	US	Yes - DocuSign BAA on file	Yes - DocuSign DPA on file	Yes - Type II annually	DocuSign sub-processors	T3 - Medium	2026-05-14	n/a - sub-processor to a sub-processor; not in customer data path

3. Aggregate counts

Tier	Vendor count

T1 - Critical	4 (AWS RDS, S3, KMS, CloudHSM)
T2 - High	6 (AWS Secrets Manager, ElastiCache, CloudFront/WAF/Shield, CloudWatch/GuardDuty, EKS, Sigstore Rekor)
T3 - Medium	4 (AWS Route 53, Postmark/SES, Stripe planned, DocuSign planned)
T4 - Low	1 (GitHub)
N/A - not currently used	2 (Cloudflare planned, Datadog planned)
Total inventoried	**17**

(Vendors whose name contains "AWS -" are counted once per service line because AWS treats each service as a separate contractual scope under its BAA, and the Phase 4 vendor_snapshots schema lists them individually.)

4. Notes on the matrix

1. **AWS as the primary T1 vendor.** Helix runs on AWS. The depth of the AWS line items reflects that AWS provides multiple discrete services under one umbrella BAA. From a customer's perspective, "Helix is hosted on AWS" is the single most important data-flow fact; the line-item detail is for assessor review.
2. **Sigstore Rekor is integrity-only.** No customer payload data is ever transmitted to Rekor; only the Ed25519-signed Merkle tree head of the Helix audit log is anchored daily (D-005). The risk tier is T2 because the integrity guarantee of the audit log depends on Rekor's availability, not because Rekor processes personal data.
3. **Email provider - single vs. dual.** Helix uses AWS SES today; Postmark remains on file as a failover. Where a deal requires a specific provider, the relationship is migrated and the matrix updated.
4. **"Not currently used" rows** are retained in the matrix for transparency so that a customer reviewing this document recognises that the planned-but-not-active vendors will become live in a controlled rollout and will be disclosed under the BAA / DPA notice provisions before activation.
5. **Diff-alert subscription** indicates whether the vendor's published terms / sub-processor list / SOC 2 cadence is monitored by the Phase 4 `vendor_snapshots` system; customers subscribed to ROPA notifications receive the diff alert.

5. Update process

The matrix is updated:

1. **On every onboarding.** A new vendor cannot be activated until a matrix row exists.
2. **On every contract material change** (e.g., AWS adds a new sub-processor, Sigstore Rekor changes its operational model).
3. **Quarterly review.** Compliance Office walks the matrix; each vendor's SOC 2, BAA, and DPA dates are verified.

4. **On customer request.** Customers may request a current snapshot at any time via sales@mabble.ai.

6. Cross-references

- BAA template: `docs/compliance/baa_template.md` (Annex C carries the sub-processor list at execution)
- Sub-processor public disclosure: `docs/compliance/sub_processors.md`
- BAA cover letter: `internal/compliance/BAA_cover_letter.md`
- DPA cover letter: `internal/compliance/DPA_cover_letter.md`
- SCC Module 2 cover letter: `internal/compliance/SCC_module_2_cover_letter.md`
- Breach notification runbook: `internal/compliance/breach_notification_runbook.md`
- ROPA Art. 30 records: `db/schema/cortex/14a_ropa_*.sql`
- Vendor snapshot data model: `db/schema/cortex/13c_vendor_snapshots.sql`

Change log

Version	Date	Change
0.1.0	2026-05-14	Initial Track C publication.