Data Residency & Data Processing Notes

Information for IT, security, and DPO review.

Hosting & sub-processors

- **Application & edge compute:** Cloudflare Workers (global edge, with region pinning available on Enterprise).
- **Database & storage:** Supabase (Postgres) hosted on AWS. SOC 2 Type II.
- **Email delivery:** Resend (transactional email).
- **Payments:** Stripe (PCI-DSS Level 1). ThermoCalc does not store card data.
- Full sub-processor list with addresses and DPA links available on request.

Data residency options

- **US (default):** Primary region us-east-1 with replica us-west-2.
- **EU:** Primary region eu-central-1 (Frankfurt). Available as a contractual option for Enterprise. No data leaves the EU region except for aggregated, anonymized telemetry.
- Region selection is set at provisioning and recorded in the Order Form.

Personal data processed

- **Account data:** name, email, organization, role.
- **Session data:** saved calculator inputs, exports, audit metadata (who/when/what).
- **Operational logs:** IP, user-agent, request paths (retained 30 days, then aggregated).
- No special-category data (health, biometric, etc.) is collected or required.

Retention & deletion

- Customer-controlled retention: 90 days, 1 year, or 7 years (audit-grade) at the org level.
- On contract termination, exportable for 90 days, then securely deleted within 30 days.
- Backups follow the same lifecycle, with deletion within 60 days of source deletion.

Encryption

- In transit: TLS 1.3 with modern ciphers; HSTS enforced.
- At rest: AES-256 (managed by hosting providers, with envelope-encrypted secrets in HashiCorp Vault-equivalent).
- Key rotation: annual for KEKs, automated for DEKs.

Cross-border transfers

For US-hosted customers, the DPA includes the EU Standard Contractual Clauses (SCCs) and a Transfer Impact Assessment summary. For EU-hosted customers, no cross-border transfer occurs in normal operation.

Incident response

- 24-hour notification SLA for confirmed security incidents affecting Customer Data.
- Post-incident report within 10 business days, including root cause and remediation.
- Annual tabletop exercise; quarterly internal review.

Available on request

- SOC 2 Type II report (under NDA).
- Penetration test summary (annual, by third-party assessor).
- SIG-Lite or CAIQ completed questionnaire.