# TOTALLY PRIVATE AI

Evidence Pack

*Your Data. Your AI. Totally Private.*

| | |
|---|---|
| **Version** | V3.0 APAC \| For security & compliance review |
| **Company** | Totally Private AI (TPAI) |
| **Use Cases** | Financial Services, Legal, Healthcare, Government |
| **Markets** | Singapore, Hong Kong SAR, Thailand & APAC |
| **Contact** | rcastillo@totallyprivate.ai |

## Key Definitions

| | |
|---|---|
| **Air-gapped** | No public internet egress. Application plane has no direct internet egress (no IGW/NAT for application subnets) and relies on private connectivity (VPC endpoints) for required cloud services. Air-gapped deployments apply to POC and Enterprise tiers. Pro and Teams are secure multi-tenant offerings with controlled access. For clarity: 'air-gapped' in this document means no public internet egress from application subnets and private service connectivity via approved endpoints; it does not imply physically disconnected hardware. |
| **Customer Data** | Prompts, file uploads, chat outputs, and any content provided by users. Stored encrypted with envelope encryption (DEKs protected by KMS). |
| **Retention** | Customer data: configurable (30-day minimum for backup/operational requirements). Audit logs: metadata only, configurable retention. |
| **Pseudonymous IDs** | User identification via HMAC-SHA256 of email address with secret key. Not reversible without key access and privileged system abuse. Re-identification requires separate access to billing systems and is controlled via role-based access. |
| **Data Residency** | Customer data processed and stored within APAC AWS regions. Available regions include Singapore (ap-southeast-1), Hong Kong (ap-east-1), Thailand (ap-southeast-7), Tokyo (ap-northeast-1), Sydney (ap-southeast-2), and others. |

## Security Posture at a Glance

- **Air-gapped:** No public internet egress; entire environment isolated
- **Encrypted:** Envelope encryption with KMS protection
- **Auditable:** Per-request logging with SIEM export
- **Framework aligned:** Mapped to Singapore PDPA, Hong Kong PDPO, Thailand PDPA, MAS TRM Guidelines, and ISO 27001 controls (not certified yet; certification roadmap available). Customer remains accountable for regulatory compliance determinations.

# Data Flow Overview

| User<br>Browser/App | VPN/SAML<br>Authentication | Gateway<br>RBAC Enforcement | Model Route<br>Bedrock/Local | Audit Logs<br>CloudWatch/SIEM |
|---|---|---|---|---|

*AIR-GAPPED ENVIRONMENT (No Public Internet Egress)*

1. **Authentication:** Client certificates (Pro) or SAML integration (Enterprise)
2. **Authorization Gateway:** RBAC enforcement before any LLM call
3. **Model Routing:** Bedrock via VPC endpoints
4. **Audit Trail:** Metadata logged to CloudWatch and S3 (no content)
5. **Data Storage:** Customer data encrypted with envelope encryption

# Deployment Models & Shared Responsibility

| Responsibility | TPAI Pro/POC | TPAI Enterprise |
|---|---|---|
| **Infrastructure** | TPAI AWS account | Customer AWS account |
| **Key Management** | TPAI-managed CMKs with strict tenant isolation | Customer-managed CMKs in customer account |
| **Data Protection Role** | TPAI is Data Processor | With Maintenance: Processor. Without Maintenance: No ongoing processor relationship |
| **Production Access** | TPAI (for operations) | Customer only (TPAI requires permission) |

# What We Guarantee Today (Beta)

- **Air-gapped application plane.** No 0.0.0.0/0 egress from app subnets; Security Groups default-deny; service access via VPC Endpoints (Interface for AWS services such as Bedrock/KMS/Logs) and AWS Gateway (for S3/DynamoDB).
- **Policy-first authorization (RBAC).** The LLM never grants privileges. The platform enforces role-based access at the gateway before any tool/LLM call. (Roadmap: optional policy-as-code engine for attribute/context rules.)
- **Least privilege, explicit tool/API allow-lists.** Each role/tenant has a defined set of callable tools/APIs; platform issues scoped, short-lived STS credentials and blocks undeclared endpoints. No long-lived model tokens on clients.
- **Data governance by default.** Per-user envelope encryption (DEKs protected by KMS CMKs) with kms:EncryptionContext binding; configurable retention (30-day minimum); optional Object Lock for legal hold.
- **Audit & export (beta).** The orchestrator emits a per-request audit event (timestamp, tenant/principal/role, model ID, route ID, token usage where available, policy decision flags, input hash). No direct identifiers in application logs. Events stream to CloudWatch (EMF) and S3 for SIEM.
- **Provider continuity.** Bedrock via Private VPC endpoints; open-weights in VPC available as controlled fallback; every inference logs vendor/model "route" for traceability.
- **No training on customer data.** Explicit no-training guarantee. AWS Bedrock models do not train on customer inputs per AWS service terms.

## AWS Bedrock Implementation Details

**What Bedrock receives:** Inference requests containing prompts and context via VPC private endpoints. May include pseudonymous user IDs for request routing. No customer metadata beyond the inference request itself.

**Retention policy:** AWS Bedrock does not store customer prompts or outputs per AWS service terms.

**Traffic routing:** All Bedrock communication via VPC Interface Endpoints; no internet transit.

# APAC Regulatory Alignment

## Singapore: Personal Data Protection Act (PDPA)

The Singapore PDPA (2012, amended 2020) is administered by the Personal Data Protection Commission (PDPC) under the Infocomm Media Development Authority (IMDA). It establishes 11 data protection obligations for private-sector organisations, with penalties of up to 10% of annual turnover or SGD 1 million (whichever is higher). TPAI implements the following technical controls that support customer PDPA compliance obligations:

- **Consent & Purpose Limitation:** TPAI processes data solely as directed by the customer (controller). No secondary use, no marketing, no data sharing. Customer defines purpose; TPAI enforces it.
- **Protection Obligation:** Air-gapped architecture with envelope encryption, RBAC enforcement, and network isolation directly addresses the PDPA requirement for reasonable security arrangements to prevent unauthorised access, use, or disclosure.
- **Retention Limitation:** Configurable retention periods with automatic deletion. Customers control how long data is held; TPAI enforces the policy.
- **Access & Correction:** Platform provides data export (JSON/CSV) and correction capabilities for customer compliance with data subject requests. Enterprise customers have direct database access.
- **Transfer Limitation (Section 26):** TPAI supports in-region deployment within Singapore (ap-southeast-1) and other APAC regions. Customer controls region selection and can enforce via AWS Service Control Policies. No cross-border transfers unless explicitly configured.
- **Data Breach Notification:** TPAI notifies customers without undue delay (target 24 hours). PDPA requires notification to PDPC within 3 calendar days for notifiable breaches; TPAI provides incident details to support customer reporting.

## Hong Kong SAR: Personal Data (Privacy) Ordinance (PDPO)

The Hong Kong PDPO (1995, amended 2012 and 2021) is enforced by the Office of the Privacy Commissioner for Personal Data (PCPD). It establishes six Data Protection Principles (DPPs) applicable to data users in both public and private sectors. TPAI implements controls that support customer PDPO compliance:

- **DPP1 – Purpose & Collection:** TPAI collects and processes data only for purposes directed by the customer. No excessive data collection; purpose limitation enforced at the platform level.
- **DPP2 – Accuracy & Retention:** Configurable retention with automatic deletion. Customer controls data lifecycle.
- **DPP3 – Use of Personal Data:** No secondary use. Customer data used solely for the AI inference purpose specified by the customer.
- **DPP4 – Security:** Air-gapped architecture, envelope encryption, and RBAC enforcement address the requirement for all practicable steps to protect personal data against unauthorised or accidental access, processing, erasure, loss, or use.
- **DPP5 – Openness:** TPAI provides this Evidence Pack, DPA templates, subprocessor lists, and security architecture documentation.

- **DPP6 – Data Access & Correction:** Platform supports data export and correction to assist customers in fulfilling data subject access requests.
- **Cloud Computing Guidance:** TPAI's architecture aligns with PCPD cloud computing recommendations including disclosure of data storage locations, subprocessor transparency, and contractual data protection requirements.

### Thailand: Personal Data Protection Act (PDPA)

Thailand's PDPA (B.E. 2562, 2019), fully enforced since June 2022, is administered by the Personal Data Protection Committee (PDPC). Enforcement has intensified significantly in 2024–2025, with over THB 21.5 million in fines across multiple cases. Penalties include administrative fines up to THB 5 million, criminal fines up to THB 1 million, and imprisonment up to one year. TPAI implements the following controls that support customer compliance:

- **Lawful Basis & Consent:** TPAI processes data solely under customer direction (contractual basis). No secondary processing. Customer manages consent from their end users.
- **Security Measures (Section 37):** Air-gapped architecture, encryption, and access controls directly address the PDPA requirement for appropriate security measures to prevent unauthorised loss, access, use, alteration, or disclosure.
- **Data Breach Notification:** TPAI supports the 72-hour PDPC notification requirement by providing customer notification within 24 hours (target) with incident details and evidence.
- **Cross-Border Transfer (Section 28):** TPAI supports in-region deployment in Asia Pacific (Thailand) ap-southeast-7, launched 2025. Also available in Singapore and Hong Kong regions. Customer controls region selection.
- **Data Subject Rights:** Access, correction, deletion, portability, and objection rights supported through platform export tools and customer controls.
- **DPO Support:** TPAI provides documentation and evidence to support customer DPO obligations, including processing records and security controls documentation.

## Financial Services Regulatory Alignment

### Singapore: MAS Technology Risk Management (TRM) Guidelines

The Monetary Authority of Singapore (MAS) TRM Guidelines (revised January 2021, with the mandatory TRM Notice effective May 2024) set risk management principles for all licensed financial institutions. TPAI implements controls that support institution assessments against MAS TRM requirements. Customer remains accountable for institution-level compliance:

- **IT Governance:** TPAI provides comprehensive security architecture documentation, risk assessment support, and controls mapping to support institution-level technology risk governance.
- **Cybersecurity:** Air-gapped architecture, defence-in-depth approach with network isolation, RBAC enforcement, envelope encryption, and audit logging address MAS TRM cybersecurity expectations.
- **IT Resilience:** Enterprise deployments support 4-hour RTO targets per MAS TRM Notice requirements. Multiple resilience patterns available (single-region with backups through active-active).
- **Third-Party Risk:** TPAI provides vendor documentation, DPA templates, security questionnaire responses, audit rights, and evidence pack to support institution third-party risk assessments.
- **Incident Reporting:** TPAI supports the 1-hour MAS incident notification requirement by providing rapid customer notification and incident details.

### Hong Kong: HKMA Cybersecurity & Technology Risk Management

TPAI implements controls that support financial institutions regulated by the Hong Kong Monetary Authority (HKMA) in meeting technology risk management requirements, including documentation, security controls mapping, and architecture details relevant to HKMA's Cybersecurity Fortification Initiative (CFI).

### Thailand: Bank of Thailand (BOT) Supervision

TPAI provides documentation to support Thai financial institutions in meeting BOT requirements for ICT risk management, vendor oversight, and data protection in AI deployments.

## Data Localization & APAC AWS Regions

TPAI leverages the extensive AWS APAC infrastructure to provide in-region data processing and storage, supporting data residency and sovereignty requirements across the region:

| AWS Region | Code | Key Markets Served |
|---|---|---|
| **Asia Pacific (Singapore)** | ap-southeast-1 | Singapore, ASEAN hub, MAS-regulated institutions |
| **Asia Pacific (Hong Kong)** | ap-east-1 | Hong Kong SAR, HKMA-regulated institutions |
| **Asia Pacific (Thailand)** | ap-southeast-7 | Thailand, BOT-regulated institutions (launched 2025) |
| **Asia Pacific (Tokyo)** | ap-northeast-1 | Japan, APPI-regulated organisations |
| **Asia Pacific (Sydney)** | ap-southeast-2 | Australia, APPs-regulated organisations |
| **Asia Pacific (Jakarta)** | ap-southeast-3 | Indonesia, OJK-regulated institutions |
| **Asia Pacific (Malaysia)** | ap-southeast-5 | Malaysia, BNM-regulated institutions (launched 2024) |
| **Asia Pacific (Seoul)** | ap-northeast-2 | South Korea, PIPA-regulated organisations |
| **Asia Pacific (Mumbai)** | ap-south-1 | India, DPDP Act regulated organisations |

- Customer controls region selection and can enforce via AWS Service Control Policies
- No cross-border transfers for processing unless explicitly configured by customer
- Enterprise deployments in customer's own AWS account provide the strongest data sovereignty posture
- Local Zone in Bangkok (ap-southeast-1-bkk-1a) available for ultra-low-latency requirements

### Broader APAC Coverage

While this Evidence Pack focuses on Singapore, Hong Kong, and Thailand as primary markets, TPAI's core security controls — air-gapped architecture, envelope encryption, RBAC enforcement, and comprehensive audit logging — provide a foundation that supports customer compliance efforts under data protection frameworks across the broader APAC region, including Japan APPI, Australia Privacy Act & APPs, South Korea PIPA, Indonesia PDP Law, Malaysia PDPA, and Philippines DPA. Customer remains accountable for jurisdiction-specific legal compliance. Detailed documentation for additional jurisdictions available on request.

### APAC Contracting

TPAI is a Delaware C-Corp. For APAC clients with concerns about US jurisdiction, TPAI is exploring regional entity structures (including potential Singapore presence) to provide locally governed contracts and data processing agreements. Target: H2 2026. Enterprise deployments in the

customer's own AWS account within APAC regions provide the strongest data sovereignty posture regardless of contracting entity.

## TPAI vs. Alternatives

| Alternative | Characteristics | Timeline/Cost |
|---|---|---|
| **Enterprise AI SaaS** | Data processed on vendor infrastructure, subject to their policies. Data may transit outside APAC region. | Immediate |
| **Cloud AI Private Endpoints** | Network isolation but processing still occurs on cloud provider's managed service | Days to weeks |
| **Build Your Own** | Full control but requires ML ops expertise, infrastructure management, ongoing maintenance burden | 6–12 months, $500K+ |
| **TPAI** | Complete deployment within customer's AWS account in APAC region, customer-controlled encryption, zero external dependencies for AI processing | Weeks not months |

## Data Portability & Exit

- Customer owns all data and encryption keys
- Standard export formats (JSON, CSV, markdown)
- No proprietary data formats
- For Enterprise deployments, customer retains full environment after contract termination

## Evidence Index

Artifacts available on request:

| Claim | How We Prove It | Artifact ID |
|---|---|---|
| **No public egress from environment** | describe-route-tables export showing no 0.0.0.0/0; NAT gateways = 0 | EP-01 |
| **VPC Endpoint scoping** | describe-vpc-endpoints (Bedrock/STS/Secrets/Logs), S3/DDB Gateway endpoints | EP-01 |
| **RBAC at gateway (LLM never authorizes)** | Role-to-permission map; sample policy (OPA/Cedar roadmap noted) | EP-07 |
| **Envelope encryption** | CMK policy with kms:EncryptionContext condition; rotation status | EP-02 |
| **Per-request audit event** | JSON/CSV sample (principal, model/route IDs, tokens, decisions); SIEM export | EP-03 |

## Legal & Privacy Summary

### Data Processing Role

TPAI acts as processor when processing personal data on customer's behalf (Pro/POC deployments; Enterprise with maintenance access). For fully customer-controlled Enterprise deployments without TPAI access, no ongoing processor relationship exists.

### Subprocessor Management

- **AWS (Infrastructure):** Compute, storage, networking services
- **Anthropic (via Bedrock):** Claude model inference only
- **OpenAI (via Bedrock):** GPT model inference only
- **Meta (via Bedrock):** Llama model inference only
- **Mistral AI (via Bedrock):** Mistral model inference only

**Customer model control:** Customers choose which models are enabled for their deployment. Organisations with specific risk requirements can restrict to Anthropic-only, open-weights-only (Llama/Mistral), or any combination. Model availability is configured per user/role via RBAC policy.

**No direct data sharing:** Model providers receive inference requests via AWS Bedrock private endpoints. No customer data flows directly to model provider infrastructure.

### Data Processing Agreements

DPA templates available on request. Standard processor terms including data minimization, purpose limitation, security requirements, and data subject rights support. Templates adaptable to Singapore PDPA, Hong Kong PDPO, and Thailand PDPA requirements. ASEAN Model Contractual Clauses (MCCs) supported for cross-border transfers where applicable.

### Breach Notification

TPAI notifies customers without undue delay (target 24 hours). Customers (as controllers) manage supervisory authority notifications (PDPC Singapore, PCPD Hong Kong, PDPC Thailand, or relevant regulator); TPAI provides incident details and evidence. Architecture supports Singapore's 3-day and Thailand's 72-hour notification timelines.

### Privileged Access & Break-Glass

TPAI production access is disabled by default and enabled only through an explicit customer-approved workflow (ticket + approval) or break-glass. Break-glass is restricted to a small on-call group, requires MFA, is time-bounded, and generates immutable audit logs (who/what/when). Post-incident review is performed and shared with the customer on request.

### Update Delivery

Production updates delivered via private connectivity channel. For customer-hosted Enterprise deployments, updates applied under customer change control.

- **Supply chain transparency:** SBOM, vulnerability scan results, and provenance attestations provided with each release.
- **Offline option:** For strict air-gap requirements, offline update packages available as commercial support option.

## Frequently Asked Questions

**Q: Exactly what data is stored where?**

A: Prompts, outputs, files, and chat history stored in OpenWebUI database (encrypted per-user) or customer S3. Audit logs in CloudWatch/S3 (metadata only, no content).

**Q: Can retention be set to zero?**
A: Customer data retention configurable with 30-day minimum for backup/operational requirements.

**Q: Which AI models are available and how are they governed?**
A: Claude Opus/Sonnet, Llama 3.1/3.2, Mistral 7B/8x7B via AWS Bedrock. Customer can restrict available models per user/role. Content filtering via AWS Bedrock Guardrails available. Model routing and decision logging for auditability.

**Q: How does deletion work with backups and legal holds?**
A: Data ages out based on retention period. Legal holds supported with AWS S3 Object Lock and treated separately from standard retention.

**Q: Who can access production and how is it approved/logged?**
A: Customer Admin has full access. TPAI accesses only with customer permission or break-glass emergencies (logged and time-bounded).

**Q: Does TPAI support Singapore PDPA transfer limitation requirements?**
A: TPAI supports deployment in Singapore (ap-southeast-1) and multiple other APAC regions. Customer controls region selection via AWS Service Control Policies. Enterprise deployments in customer accounts provide the strongest data sovereignty posture.

**Q: How does TPAI support MAS TRM compliance for banks?**
A: TPAI provides architecture documentation, security controls mapping, audit evidence, and vendor risk documentation that support institution assessments against MAS TRM Guidelines. The air-gapped architecture implements controls that address TRM expectations for access control, cryptography, network security, and IT resilience (4-hour RTO supported). Customer remains accountable for institution-level compliance.

**Q: Can TPAI deploy in the new Thailand AWS region?**
A: Yes. The Asia Pacific (Thailand) region (ap-southeast-7) launched in 2025 and is supported for TPAI deployments, enabling in-country data residency for Thai organisations.

**Q: What's your uptime target?**
A: 99.9% for standard deployments, 99.99% available with Enterprise SLA. Incident response included in maintenance plan.

**Q: Is penetration testing available?**
A: Air-gapped architecture significantly limits attack surface. External penetration testing scheduled for Q2 2026.

# Business Continuity & Incident Response

## Incident Response

TPAI maintains incident detection, containment, and customer notification processes. For security incidents affecting customer data, we notify customers without undue delay (target: 24 hours) and provide periodic updates. Customers handle regulatory notifications (PDPC Singapore, PCPD Hong Kong, PDPC Thailand, or applicable authority); TPAI provides technical details and evidence.

## Business Continuity

Enterprise deployments support multiple resilience patterns based on customer requirements (single-region with backups, pilot light, warm standby, active-active). Target RTO/RPO configured per customer deployment.

### Pre-Certification Assurance

While formal certifications are in progress, TPAI implements compensating controls: self-assessment against ISO 27001 Annex A, quarterly security reviews, vulnerability scanning in CI/CD pipeline, and immutable audit logging. Gap analysis and remediation plans available on request.

## Certification Status & Roadmap

| | |
|---|---|
| **Current Status** | Self-attestation against ISO 27001 controls. Controls mapped to Singapore PDPA, Hong Kong PDPO, Thailand PDPA, and MAS TRM requirements |
| **Q2 2026** | SOC 2 Type I assessment initiated |
| **Q3 2026** | ISO 27001 certification process (target) |
| **Q4 2026** | SOC 2 Type II (target) |

*Control alignment summaries and gap analysis available on request.*

## Regulatory Framework Coverage Summary

| Framework | Jurisdiction | TPAI Alignment |
|---|---|---|
| **PDPA (Personal Data Protection Act)** | Singapore | 11 obligations: consent, purpose limitation, protection, retention, access, correction, accuracy, transfer limitation, breach notification, accountability, DPO |
| **PDPO (Personal Data Privacy Ordinance)** | Hong Kong SAR | 6 Data Protection Principles: purpose/collection, accuracy/retention, use, security, openness, access/correction |
| **PDPA (Personal Data Protection Act)** | Thailand | Lawful basis, consent, security measures, breach notification (72hr), cross-border transfer, data subject rights, DPO |
| **MAS TRM Guidelines & Notice** | Singapore (Financial) | IT governance, cybersecurity, IT resilience, third-party risk, incident reporting (1hr), 4-hour RTO |
| **MAS Notice on Cyber Hygiene** | Singapore (Financial) | Administrative account security, patching, baseline standards, network security, anti-malware, authentication |
| **HKMA CFI** | Hong Kong (Financial) | Cybersecurity Fortification Initiative: assessment, simulation, intelligence sharing |
| **BOT ICT Risk Management** | Thailand (Financial) | ICT risk governance, vendor oversight, data protection in financial services |
| **ISO 27001** | International | Annex A controls self-assessment; certification targeted Q3 2026 |
| **NIST 800-53** | International | Controls mapped to access control, audit, encryption, and incident response families |

*Your Data. Your AI. Totally Private.*