TOTALLY PRIVATE AI

Evidence Pack

Your Data. Your AI. Totally Private.

Version	V3.0 ME | For security & compliance review
Company	Totally Private AI (TPAI)
Use Cases	Financial Services, Legal, Healthcare, Government
Markets	Kingdom of Saudi Arabia, UAE & GCC
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 GCC-region AWS infrastructure. Available regions: Middle East (Bahrain) me-south-1, Middle East (UAE) me-central-1. KSA region anticipated 2026.

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 NCA ECC-2 controls, SAMA CSF domains, KSA PDPL, UAE PDPL, and ISO 27001 controls (not certified yet; certification roadmap available). Customer remains accountable for regulatory compliance determinations.

Data Flow Overview

User Browser/App	VPN/SAML Authentication	Gateway RBAC Enforcement	Model Route Bedrock/Local	Audit Logs 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.

Middle East Regulatory Alignment

Kingdom of Saudi Arabia: PDPL Alignment

The Saudi Personal Data Protection Law (PDPL), enforced since September 2024 under the oversight of the Saudi Data and Artificial Intelligence Authority (SDAIA), establishes comprehensive data protection requirements with extraterritorial reach. TPAI implements the following technical controls that support customer PDPL compliance obligations:

- **Data Minimization (Article 10):** Only necessary data processed; configurable retention periods; automatic deletion
- **Security of Processing:** Encryption in transit and at rest; access controls aligned with NCA cryptographic standards (NCS-1:2020); regular security assessments
- **Data Subject Rights (Articles 14–19):** Customer controls all personal data. For Pro/POC: TPAI provides data export tools and deletion capabilities. For Enterprise: Customer has direct database access. Data portability via standard formats (JSON/CSV). Deletion propagates to backups within retention period.
- **Cross-Border Transfer Controls:** TPAI implements in-region data processing within GCC AWS regions (Bahrain, UAE). Current production options: Bahrain (me-south-1) and UAE (me-central-1). For KSA government entities requiring strict in-kingdom data residency, TPAI's architecture is designed to support in-kingdom deployment once the AWS KSA region (announced 2026) is available and customer validation criteria are met. Transfer risk assessments available per SDAIA Transfer Regulations (August 2024).

United Arab Emirates: Federal PDPL Alignment

The UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection establishes data protection requirements for entities processing personal data of UAE residents. TPAI implements controls that support customer UAE PDPL obligations:

- **Consent & Legal Basis:** TPAI processes data solely as directed by the customer (controller). No secondary use of customer data.
- **Data Subject Rights:** Access, correction, deletion, and portability supported through platform capabilities and standard export formats.
- **Automated Decision-Making (Article 12):** TPAI provides audit logging of all AI interactions, supporting customer obligations around transparency of automated processing.
- **DIFC & ADGM:** For clients operating within Dubai International Financial Centre or Abu Dhabi Global Market free zones, TPAI implements controls that support the additional data protection requirements of DIFC Law No. 5 of 2020 and ADGM Data Protection Regulations 2021. Customer remains accountable for regulatory classification and reporting.

Financial Services: SAMA CSF, CBUAE & DFSA Alignment

TPAI implements technical controls that support financial institutions subject to the SAMA Cyber Security Framework (CSF), the Central Bank of the UAE (CBUAE) regulatory requirements, and the Dubai Financial Services Authority (DFSA) for DIFC-regulated firms. Customer remains accountable for institution-level compliance determination and regulatory reporting:

- **SAMA CSF Cybersecurity Governance (Domain 1):** TPAI provides controls documentation, audit evidence, and security architecture details that support institution-level governance and board reporting obligations.
- **SAMA CSF Cybersecurity Defense (Domain 2):** Air-gapped architecture, envelope encryption, RBAC enforcement, and network isolation directly address access control, cryptography, and network security management controls.
- **SAMA CSF Third-Party Cybersecurity (Domain 3.4):** Comprehensive vendor documentation, DPA, security questionnaire responses, and evidence pack support third-party risk assessment requirements.
- **CBUAE Banking Data Protection:** Customer-managed deployments ensure banking data remains under institution control with no external access by default.
- **DFSA (DIFC):** TPAI implements controls that support DIFC-regulated firms' technology risk and outsourcing requirements through vendor documentation, audit evidence, and architecture-level controls mapping.

NCA Essential Cybersecurity Controls (ECC-2) Alignment

The National Cybersecurity Authority's Essential Cybersecurity Controls (ECC-2, updated 2024) are mandatory for government entities and organisations operating critical national infrastructure in KSA. TPAI implements technical controls that support customer compliance across multiple ECC-2 domains. Final control applicability depends on customer classification, environment scope, and NCA assessment.

ECC-2 Domain	TPAI Control
Cybersecurity Governance (1-1 through 1-4)	Security architecture documentation, risk assessment support, incident response procedures, and compliance evidence pack provided.
Cybersecurity Defense (2-1 through 2-12)	Air-gapped network isolation, RBAC access control, envelope encryption (aligned with NCS-1:2020 cryptographic standards), vulnerability scanning in CI/CD, and comprehensive audit logging.
Cybersecurity Resilience (3-1 through 3-2)	Business continuity patterns (single-region with backups through active-active), incident response with 24-hour customer notification target.
Third-Party & Cloud Cybersecurity (4-1 through 4-2)	Vendor documentation, subprocessor transparency, DPA templates, and controls that support NCA Cloud Cybersecurity Controls (CCC) requirements for cloud deployments.

Detailed control-by-control mapping against all 114 ECC-2 controls available on request.

Data Localization & Residency

- GCC customer data processed and stored within Middle East AWS regions: Bahrain (me-south-1) and UAE (me-central-1)
- KSA in-kingdom residency: Architecture designed to support in-kingdom deployment once the AWS KSA region (announced 2026) is available and customer validation criteria are met. Current production options: Bahrain (me-south-1), UAE (me-central-1). Region availability last reviewed: February 2026.
- No cross-border transfers for processing unless explicitly configured by customer
- Customer controls region selection and can enforce via AWS Service Control Policies
- Data residency compliance aligned with SDAIA/NDMO data localisation guidance

Middle East Regulatory Context

TPAI provides ICT software/services that may be used by regulated entities to support internal knowledge work while applying strict security controls (access control, encryption, audit logging, and egress restriction).

Under the SAMA CSF, financial institutions assess whether TPAI is an ICT third-party service provider for their cybersecurity and vendor risk management processes; TPAI supports these assessments with contractual and technical documentation.

Under emerging AI governance frameworks in the region, risk classification depends primarily on the customer's intended use. TPAI does not develop or place a general-purpose AI model on the market; it integrates and controls access to third-party models. Customers remain responsible for use-case classification and any obligations tied to their deployment context.

GCC Contracting

We understand GCC clients may have concerns about US jurisdiction and data sovereignty. TPAI is partnering with regional entities to provide GCC-domiciled contracting so that regional contracts can be governed by KSA or UAE law, with local data processing agreements and support. Target: H2 2026. Enterprise deployments in the customer's own AWS account within GCC 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 GCC 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 GCC 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 KSA PDPL and UAE PDPL requirements.

Breach Notification

TPAI notifies customers without undue delay (target 24 hours). Customers (as controllers) manage supervisory authority notifications (SDAIA, UAE Data Office, or relevant regulator); TPAI provides incident details and evidence.

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: What does Bedrock receive?
A: Inference requests containing prompts and context. May include pseudonymous user IDs for request routing. No customer metadata beyond the inference request itself.

Q: Does TPAI support KSA data localisation requirements?
A: TPAI currently deploys in Middle East AWS regions (Bahrain, UAE). For KSA government entities requiring strict in-kingdom residency, the architecture is designed to support in-kingdom deployment once the AWS KSA region is available. Customer-managed Enterprise deployments can enforce region selection via AWS Service Control Policies. Region availability last reviewed: February 2026.

Q: How does TPAI support SAMA CSF compliance for banks?
A: TPAI provides architecture documentation, security controls mapping, audit evidence, and vendor risk documentation that support institution assessments against SAMA CSF domains. The air-gapped architecture implements controls that address multiple SAMA CSF Level 3 maturity requirements. Customer remains accountable for institution-level compliance determination.

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 (SDAIA, UAE Data Office, SAMA, 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 KSA PDPL, NCA ECC-2, and SAMA CSF 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
PDPL (Personal Data Protection Law)	KSA	Data minimisation, encryption, data subject rights, cross-border transfer controls
UAE PDPL (Federal Decree-Law 45/2021)	UAE	Processing controls, data subject rights, automated decision transparency
DIFC Data Protection Law No. 5/2020	DIFC (Dubai)	Enhanced AI transparency, data protection impact assessments
ADGM Data Protection Regulations 2021	ADGM (Abu Dhabi)	Controller/processor obligations, cross-border safeguards
Bahrain PDPA (Law No. 30 of 2018)	Bahrain	TPAI implements controls that support compliance; customer data hosted in Bahrain (me-south-1)
Qatar Data Privacy Law (Law No. 13 of 2016)	Qatar	TPAI implements controls that support compliance; nearest region: Bahrain (me-south-1)

SAMA Cyber Security Framework (CSF)	KSA (Financial)	Governance, defence, resilience, third-party controls across all CSF domains
NCA ECC-2 (2024)	KSA	114 cybersecurity controls: governance, defence, resilience, cloud security
NCA Cloud Cybersecurity Controls (CCC)	KSA	Cloud-specific security controls for government and CNI organisations
DFSA Technology & Outsourcing	DIFC (Financial)	Technology risk management, outsourcing controls for DIFC-regulated firms
CBUAE	UAE (Financial)	Banking data protection, technology risk management
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.