TOTALLY PRIVATE AI

AI for Enterprise Financial Services

Private AI infrastructure. Deployed in your cloud. Under your control.

AI adoption is already happening inside your firm. The question is whether you control it.

> *Presented in partnership with* **[Partner Name]** | *[Partner logo]*
> *Remove this box for direct TPAI distribution.*

A PROBLEM WITH NO GOOD ANSWER

If you are responsible for data security in a regulated financial institution, you already know the trap. Adopt public AI tools, and the risk surface expands with every prompt. Client data, deal flow, and MNPI reach a third-party server outside your environment. Your team gains capability fast. **and your compliance posture gets harder to defend.**

What if you refuse? Something worse happens. Your teams use ChatGPT anyway. On personal devices. On home networks. With client names, deal terms, and portfolio data in the prompt. **You have not prevented AI adoption. You have just lost visibility over it.**

> **The board asks why competitors are moving faster. The regulator asks why sensitive data touched an AI vendor. Both questions land on the same desk.**
> *There is no version of this where "do nothing" or "block everything" ends well. The only question is whether AI adoption happens under your governance or outside it.*

In either case, the underlying problem is the same. Public AI platforms create a prompt and response record on vendor infrastructure. Whether that activity is sanctioned or shadow, **that record is outside your environment, outside your control, and outside your clients' consent.**[1]

Shadow AI is not a policy problem. It is a tooling vacuum.

THE THIRD PATH

You don't need a new AI strategy.
You need a boundary.
You need governance.
You need evidence.

Totally Private AI (TPAI) Enterprise is not a safer way to use public AI. **It is a different architecture entirely.** TPAI Enterprise is a private AI platform deployed directly into your own AWS account. Your infrastructure, your keys, your data.

Public AI is adoption without control. An internal build is control without speed. **TPAI is adoption with control, at speed.**

Your TPAI environment is your AWS account and VPC boundary, deployed and governed entirely by your team. Not a vendor's cloud. Not a shared tenant. **Your environment, your encryption keys, your access controls.**

Every prompt. Every response. Every analysis. Encrypted at the application layer, per user, using AWS KMS with customer-managed keys. TPAI operators have no routine access to your content. There is no public internet egress path. Your data does not leave your environment.

Other vendors manage your data carefully. **TPAI does not manage it at all.** We deploy the infrastructure. You own everything that runs on it.

Build vs. Buy

A comparable internal build takes 18 to 36 months and typically exceeds €1.5M, with ongoing engineering cost to maintain and secure it. **A TPAI proof of concept is live in 1 to 2 weeks. Full enterprise deployment in under 30 days.**

The Cost of Waiting

At €90 per hour per employee, a 30-day delay costs a 100-person team **€180,000** in lost productivity. Every month of delay is that cost again, compounding, while competitors who have already deployed extend their lead.

Your job is to keep client data out of unnecessary custody. With TPAI, that record is never created outside your boundary in the first place.

The safest disclosure response is the one you never have to make.

Your Data. Your AI. Totally Private.

HIGH-VALUE WORKFLOWS

Capability	What your team can do
Internal Knowledge Search	Search policies, prior investment decisions, research archives, and committee history instantly, with nothing leaving your environment
Client Communications	Draft quarterly letters, LP updates, and portfolio reports with full client context and strict confidentiality boundaries
Compliance and Risk	Map regulatory procedures, prepare examination packs, and produce audit documentation with a complete internal trail
Deal Analysis	M&A due diligence, CIM review, and valuation work with MNPI confined to your perimeter throughout
Investment Research	Summarise filings, earnings transcripts, and market data with your proprietary models and annotations kept private

Every workflow runs inside your environment. Client data never touches a third-party server.

WHY NOT THE ALTERNATIVES

Approach	The limitation
Public AI (OpenAI, Anthropic)	Data processed on vendor infrastructure. Retained. Accessible under legal process.
Protected workspace platforms	Still third-party managed. The provider holds data and remains subject to legal process.
Internal cloud build	Full control. Also: 18 to 36 months, €1.5M+, and ongoing engineering cost with no guaranteed compliance outcome.
TPAI Enterprise	Deployed in your AWS account. Your keys. Your access controls. Your region. TPAI holds nothing. Operational in weeks.

The choice is not between AI and security. It is between architectures.

SECURITY ARCHITECTURE

Control	What it means for you
Network Isolation	No public internet egress. No outbound path means no exfiltration path.
Per-User Encryption	Application-layer encryption per user via AWS KMS with customer-managed keys. TPAI has no decryption access.
Operator Access	No routine TPAI access to your content. Any support engagement requires your explicit authorisation and is fully logged.
Data Residency	Deploy in AWS regions globally, including all EU regions (subject to model availability). Your data stays in the jurisdiction you choose.
Model Training	Customer content is not used to train base models under the AWS Bedrock deployment model and service terms. [2]
Compliance Alignment	Architecture mapped to GDPR, DORA, and ISO 27001 controls. EU AI Act alignment in progress. Evidence pack available under NDA.

Model training: customer content is not used to train base models. See Note 2 below.

Evidence pack covering GDPR, DORA, and ISO 27001 controls is available under NDA before you commit to a proof of concept.

Notes

[1] The New York Times Company v. Microsoft Corporation et al., No. 1:23-cv-11195 (S.D.N.Y. 2023). In discovery, OpenAI produced prompt and response data including from sessions the user had deleted. For AWS Bedrock data handling and retention terms, see: aws.amazon.com/bedrock/faqs

[2] AWS Service Terms, Section 50.10 (Amazon Bedrock): "Amazon Bedrock does not use your prompts and completions to train the base models." See: aws.amazon.com/service-terms

HOW WE WORK TOGETHER

Designed for security leaders who need to say yes to AI without creating a new audit surface.

Proof of Concept: A dedicated TPAI-hosted proof of concept. 20 to 30 users, 6 weeks, real workflows. You evaluate the platform on live use cases before any broader commitment. Evidence pack covering GDPR, DORA, and ISO 27001 controls is available before you commit.

Enterprise Deployment: 100 to 250+ seats deployed into your AWS account, with full onboarding, training, and ongoing maintenance. Your team runs the AI. We run the infrastructure.

Built by security architects with 25+ years of enterprise experience across regulated industries. Technical deployment is typically 4 to 6 weeks, subject to your security review and procurement timeline.

Next Step: 30 Minutes

See the architecture. Review the security controls. Understand exactly what you are deploying and what you are not exposing.

If you are evaluating AI for regulated workflows, start with a 6-week proof of concept in a dedicated private environment.

Book: calendly.com/rcastillo-totally-private

Email: rcastillo@totallyprivate.ai

Your Data. Your AI. Totally Private.