enclaive

FINANCIAL SERVICES BRIEF

2026

REGULATED FINANCIAL SERVICES

Top 5 Confidential Computing Use Cases in Financial Services

A briefing for regulated workloads that need data-in-use protection, customer-held keys, workload attestation, and evidence for cloud, AI, and third-party review

Confidential Computing | 3D Encryption at Runtime | Customer-Held Keys | Workload Identity Management | Attestation

Regulation | DORA | GDPR | EU AI Act | MiCA | PSD2 | NIS2 | ECB Cloud Guide | National Implementations

PAGES

7

READING TIME

~ 9 min

EXECUTIVE SUMMARY

Who this briefing is for

This document is written for European financial-services teams that need a common starting point for regulated cloud, AI, data, and third-party workload review.

Primary audience

For teams accountable for regulated workloads, external operators, AI usage, and key-control decisions

CISO | CIO / CTO | GRC | CLOUD | PLATFORM | DATA | AI

Banks, payment providers, fintechs, market-infrastructure providers, and digital-asset service providers

What your teams get

- A short list of workload categories to review before cloud approval, vendor approval, AI rollout, or key-management change
- A shared starting point for security, cloud, AI, compliance, procurement, and risk workshops

EU BASELINE

Regulatory baseline

DORA and GDPR provide the EU baseline. ECB cloud expectations matter for banks under ECB supervision

REGULATORY OVERLAYS

Workload overlays

EU AI Act, MiCA, PSD2, PCI DSS, AML/KYC rules, and local law enter the review based on workload, data type, service, and entity scope

REVIEW FOCUS

Control focus

The recurring review points are data exposure during processing, third-party operation, key custody, runtime integrity, and reusable evidence

How to use it

Screen
Use the Top 5 as a first screening list across fraud, payments, post-trade, KYC, AI, and adjacent regulated workloads

Select
Choose the first wave by sensitivity, operational importance, and evidence pressure

Define controls
Set the data-in-use risk, key-control model, and attestation requirement

Decision output
Document the evidence pack, owner, and approval path before production.

Prepared in 2026 for regulated-cloud, cybersecurity, compliance, platform, and AI discussions. This briefing is not legal advice and does not state that enclaive alone creates compliance. Validate final scope with legal, risk, and supervisory-affairs teams.

EXECUTIVE BASELINE

The regulation points to workload-level proof

Review teams usually need a clear answer on four points: sensitive-data exposure, third-party operation, key custody, and reusable evidence. Regulators require technical proof over policies and contractual agreements.

DORA and GDPR

ICT risk, outsourcing, processor control, encryption, security by design, and security of processing remain the main EU baseline

ECB cloud expectations

For banks under ECB supervision, cloud reviews focus on governance, data security, monitoring, auditability, and exit planning

EU AI Act and sector overlays

AI Act, MiCA, PSD2, PCI DSS, and AML/KYC requirements enter the review based on entity, workload, data type, and use

Top five use cases to review

Rank	Use case	Regulatory lens	Control pattern
1	Fraud and AML analytics with third-party tools	DORA third-party risk, GDPR, AML/KYC	Confidential Analytics with attested input and result paths
2	Payment processing, tokenization, and signing	DORA, PSD2, PCI DSS, GDPR	vHSM, Vault, confidential execution, protected authorization logic
3	Post-trade, settlement, custody, and corporate actions	DORA critical services, outsourcing, GDPR	Confidential Databases, Confidential Analytics, vHSM
4	Shared KYC, identity verification, and onboarding	GDPR, DORA third-party risk, AML/KYC	Attested matching, screening, and identity-data processing
5	Regulated AI inference, RAG, and model-context processing	EU AI Act, GDPR, DORA	Garnet, eMCP, Nitride, Vault, confidential RAG

Additional workload patterns to evaluate next

Rank	Use case	Regulatory lens	Control pattern
6	Critical cloud and Kubernetes workloads	DORA, ECB cloud, GDPR	Confidential pods, workload identity, attestation, no-attest-no-key
7	Customer-held keys and virtual HSM modernization	DORA cryptographic controls, ECB cloud, payment controls	vHSM, Vault, Nitride, attested key release
8	Confidential databases for customer and transaction data	GDPR Article 32, DORA, ECB data security	Confidential Databases, Buckypaper, Dyneemes, Vault
9	Attested CI/CD and software signing keys	DORA ICT risk, supply-chain risk, incident evidence	Attested runners, protected deploy tokens, vHSM signing
10	Crypto custody and regulated digital asset services	MiCA, DORA, AML, local implementation	Attested signing, customer-held keys, runtime isolation
11	Regulatory reporting data hubs and evidence automation	DORA incident reporting, register of information, GDPR, ECB auditability	Attested data pipelines, protected reporting data, control evidence packs

AI Act scope is driven by intended purpose and risk class. Creditworthiness for natural persons, access to essential services, and certain insurance uses need a separate EU AI Act review.

FIRST REVIEW WAVE

Start with the five strongest regulated workload candidates

These cases combine sensitive processing, third-party or shared operation, key material, and audit pressure, making them the fastest path to prove confidential computing value in regulated financial services.

1 Fraud and AML analytics

REVIEW POINT

Analytics vendors and shared models need sensitive datasets, creating processor, outsourcing, and confidentiality exposure.

CONTROL PATTERN

Confidential Analytics processes approved inputs in attested environments and limits raw-data exposure.

2 Payments, tokenization, and signing

REVIEW POINT

Payment platforms combine transaction criticality, signing keys, credentials, fraud exposure, and personal data.

CONTROL PATTERN

vHSM, Vault, Nitride, and confidential execution protect keys, tokens, credentials, and authorization logic.

3 Post-trade and custody processing

REVIEW POINT

Settlement, custody, and corporate-actions workflows share positions, client identifiers, instructions, and reference data.

CONTROL PATTERN

Confidential Databases, Confidential Analytics, and vHSM protect multi-party processing and signing operations.

4 Shared KYC and onboarding

REVIEW POINT

KYC reuse reduces friction, while raw-data sharing raises privacy, vendor, and outsourcing questions.

CONTROL PATTERN

Confidential Analytics, Nitride, and Vault support attested matching, screening, and verification.

5 Regulated AI inference and RAG

REVIEW POINT

When AI enters credit, risk, fraud, service, or advisory workflows, training data, context, inference data, model access, and key control need proof.

CONTROL PATTERN

Garnet, eMCP, Nitride, Vault, and confidential RAG protect prompts, retrieval, inference, and runtime integrity.

Executive filter

- High sensitivity during processing.
- External operator or vendor access.
- Keys, tokens, or signing material in scope.
- Evidence needed for audit, incident review, or supervision.

EXTENSION REVIEW

Review adjacent cases after the top five are scoped

These workload patterns are natural next candidates because they reuse the same control primitives: attested runtime identity, protected key release, reduced privileged access, and evidence that can support audit or supervisory review.

6 Critical cloud and Kubernetes workloads

REVIEW POINT

Provider, platform, support, and cluster-admin access becomes harder to justify when critical services process sensitive data.

CONTROL PATTERN

Dyneemes, eMCP, Nitride, and Vault bind workload execution and secret release to measured runtime state.

7 Customer-held keys and virtual HSM

REVIEW POINT

Key custody affects sovereignty, outsourcing, payment flows, and auditability.

CONTROL PATTERN

vHSM, Vault, and Nitride support customer-held keys, attestation-gated release, and key-use evidence.

8 Confidential databases

REVIEW POINT

Customer, account, payment, KYC, AML, and trading data remain exposed during query execution and privileged runtime paths.

CONTROL PATTERN

Confidential Databases, Buckypaper, Dyneemes, and Vault protect database execution and bind secrets to attestation.

9 Attested CI/CD and signing keys

REVIEW POINT

Compromised runners, deploy tokens, or signing keys can create material ICT risk.

CONTROL PATTERN

Nitride verifies runners before Vault or vHSM releases deploy tokens and signing keys.

10 Crypto custody and digital assets

REVIEW POINT

Private-key misuse, unauthorized signing, and custody continuity sit at the center of regulated digital asset services.

CONTROL PATTERN

vHSM, Vault, Nitride, and confidential execution support attested signing and customer-held keys.

11 Regulatory reporting data layer

REVIEW POINT

Incident reporting, ICT third-party registers, audit files, and supervisory packs depend on accurate, protected, and traceable data pipelines.

CONTROL PATTERN

Attested reporting pipelines, protected evidence stores, and key-release logs support repeatable reporting and audit review.

PRACTICAL ADOPTION

Run a first-wave review before a broad rollout

Choose a few workloads with sensitive processing, external operation, AI scope, or key-control friction. Define the evidence pack before production approval.

1

Classify

Rank workloads by criticality, data sensitivity, outsourcing, cloud target, AI scope, and key custody.

2

Select

Pick two to five workloads where approval, audit, or supervisory evidence is already a constraint.

3

Attest

Bind runtime identity, integrity, and secret release to measured workload state.

4

Evidence

Package attestation events, key decisions, denied access, diagrams, and control mappings.

Suggested first review

Assess fraud or AML analytics, payments, post-trade processing, shared KYC, and regulated AI against the Top 5 control patterns, then review the additional cases as extensions.

Discuss the first regulated workload

Primary references

Regulation (EU) 2022/2554 (DORA): ICT risk management, incident reporting, resilience testing, ICT third-party risk, and application from 17 January 2025.

Commission Delegated Regulation (EU) 2024/1774: DORA RTS for ICT risk management, including encryption and cryptographic controls.

Commission Delegated Regulation (EU) 2024/1773, Commission Delegated Regulation (EU) 2025/532, and Commission Implementing Regulation (EU) 2024/2956: ICT third-party policy, subcontracting assessment, and the register of information.

Commission Delegated Regulation (EU) 2025/301 and Commission Implementing Regulation (EU) 2025/302: DORA major ICT incident reporting content, timelines, forms, and procedures.

ECB final Guide on outsourcing cloud services and ECB cloud guide PDF: supervisory expectations and good practices for banks under ECB supervision.

Regulation (EU) 2016/679 (GDPR): data protection by design, processor governance, and security of processing.

Regulation (EU) 2023/1114 (MiCA): scope-dependent overlay for crypto-asset services and regulated digital asset activity.

Regulation (EU) 2024/1689 (AI Act), European Commission AI Act timeline, and European Commission AI Act FAQ: scope-dependent AI obligations and progressive application through 2027.

CONFIDENTIAL COMPUTING WITH ENCLAIVE

What is confidential computing with enclaive

Confidential computing protects data while workloads process it. enclaive adds a control plane, customer-held keys, workload attestation, and audit evidence around that runtime.

CONTROL PLANE

eMCP

Set attestation policy, control key release, and keep evidence across clouds, Kubernetes, AI workflows, and regulated applications.

One governance plane for selected workloads, keys, runtime identity, and evidence.

LAYER 03 / WORKLOADS

Run regulated applications and data services

Use the same control model for AI, databases, collaboration, software delivery, and existing workloads.

Garnet
Policy-controlled LLM and RAG usage with protected prompts, context, retrieval, and inference paths.

Confidential Databases
MariaDB, PostgreSQL, MongoDB, and Redis with data protected during query execution.

Confidential Nextcloud
Collaboration workloads with reduced infrastructure-operator exposure.

Confidential GitLab
Source code and CI/CD workloads isolated from platform administration paths.

LAYER 02 / RUNTIMES

Move workloads into confidential execution

Run existing VMs, Kubernetes workloads, and application components inside hardware-backed execution environments. Without code changes.

Buckypaper
Confidential virtual machines for existing workloads and regulated applications.

Dyneemes
Confidential Kubernetes for pods and clusters across selected cloud environments.

LAYER 01 / KEYS AND IDENTITY

Release secrets only to verified workloads

Key use, identity, and runtime integrity are bound to measured workload state.

vHSM
Cloud-scale cryptographic operations with a customer-controlled key model.

Vault
Cross-cloud secret management for keys, tokens, and workload secrets.

Nitride
Workload identity and attestation before secrets or keys are released.

Data in use
Hardware-backed runtime isolation for sensitive processing.

Key control
Secrets and keys released only to approved workload state.

Evidence
Attestation and policy records for audit and supervisory review.

Make regulated cloud, AI, and data workloads provable.

enclaive helps financial-services teams run selected workloads with data-in-use protection, customer-held keys, and attestation evidence across cloud, Kubernetes, AI, and third-party environments.

OFFICE

enclaive GmbH
Philipp-Keim-Str. 1
65719 Hofheim a. Ts.
Germany

CONNECT

contact@enclaive.io
www.enclaive.io

NEXT STEP

Book a regulated workload assessment with our solutions team.