

CUSTOMER CASE STUDY · FINANCIAL SERVICES

Sovereign by Design: How Meridian Nordbank Rebuilt for DORA

A tier-two European bank migrated 1,400 workloads and its entire AI estate onto UPC Sovereign Cloud — meeting DORA, NIS2, and GDPR obligations without surrendering control of its data, its keys, or its operations.

INDUSTRY

**Banking & Capital
Markets**

REGION

Germany & Nordics

PLATFORM

UPC Sovereign Cloud

DEPLOYMENT

Dedicated single-tenant

1,400+

Production workloads
migrated in 9 months

100%

Data, keys and
administration held in-
jurisdiction

63%

Reduction in mean time
to resolution

31%

Lower run-rate versus
prior hyperscaler estate

THE CUSTOMER

A regional bank with pan-European obligations

Meridian Nordbank is a tier-two European banking group serving 2.3 million retail and commercial customers across Germany, Denmark and Sweden, with roughly €48 billion in assets under management.

Over the previous six years the bank had pushed most of its non-core estate — analytics, customer engagement, fraud scoring, developer tooling — onto two public hyperscalers. Core banking remained on an ageing VMware footprint in two leased data-centre halls outside Frankfurt.

By early 2025 that arrangement was untenable. The Digital Operational Resilience Act (DORA) had come into force, NIS2 transposition was tightening, and the bank's own supervisory college had begun asking pointed questions about concentration risk, exit plans and third-country access to customer data. At the same time, the data science function wanted GPU capacity for credit-risk and financial-crime models trained on live customer records — data legal would not permit to leave the jurisdiction.

THE CHALLENGE

Four pressures converging at once

Regulatory exposure the bank could not evidence away

DORA Article 28 required documented, testable exit strategies for every critical ICT provider. The bank could not produce them for its hyperscaler contracts, and could not demonstrate to supervisors who — across which legal entities and which jurisdictions — held administrative access to production systems.

No control of encryption keys or audit trail

Keys were managed inside provider-operated services. Audit logs were provider-generated, provider-retained, and incomplete for the administrative actions the bank most needed to evidence. Under supervisory scrutiny, trusting a provider attestation was no longer an acceptable answer.

An AI programme blocked at the data boundary

Fraud and credit models needed GPU clusters. Every available option involved either shipping customer data across borders or accepting shared infrastructure with opaque tenancy — both vetoed. The programme had stalled for eleven months.

Legacy that could not simply be rewritten

Core banking, treasury and settlement ran on VMware and Oracle stacks with a decade of accumulated integration. Any sovereign destination had to host them as-is, alongside modern container and AI workloads, without a rewrite.

THE SOLUTION

A dedicated sovereign perimeter, built to the bank's jurisdiction

UnitedLayer deployed UPC Sovereign Cloud as a dedicated, single-tenant private cloud across two German availability zones with an in-region recovery site. Every layer — compute, storage, network, security — is provisioned exclusively for the bank, inside its chosen sovereign boundary.

What was deployed

UPC Sovereign Core

Fully managed private cloud in-region, running multi-hypervisor across VMware and KVM so core banking and Oracle estates lifted across unchanged while new workloads landed on open virtualization.

UPC AI-Optimized Sovereign Cloud

Dedicated GPU clusters inside the sovereign perimeter, with encrypted data pipelines for training and inference, plus EU AI Act mapping and data-lineage documentation for the fraud and credit-risk models.

UPC Secure Multi-Cloud Orchestration

A single control plane spanning the sovereign estate and the residual public cloud footprint, with policy-as-code governance determining where each workload is permitted to run.

Native Backup & DRaaS

Integrated backup and disaster recovery with immutable copies held in-jurisdiction, giving the bank the tested, evidenced resilience posture DORA requires.

How sovereignty was established

DIMENSION	WHAT THE BANK NOW HOLDS
Data sovereignty	Data resides in Germany, subject to German and EU law only. No hyperscaler access; no cross-border replication without contracted consent.
Operational sovereignty	Administration restricted to vetted regional personnel under residency-specific access controls. BCDR built in and exercised in-jurisdiction.
Digital sovereignty	The bank owns encryption keys, access policies and the full audit trail, enforced through centralized policy-as-code governance.
Compliance posture	Pre-certified alignment across GDPR, DORA, NIS2, BSI C5, KRITIS and ISO 27001, with a dedicated compliance advisory team tracking regulatory change.

THE DIFFERENTIATOR

Intelligence built into the sovereign perimeter

Most sovereign offerings deliver isolation and stop there, leaving the customer to bolt on monitoring, automation and remediation from elsewhere — often from tools that phone home across the very boundary the architecture exists to protect.

UPC Sovereign Cloud ships with a native intelligence layer: Unified Observability, AIOps and Agentic Orchestration built directly into the platform. For Meridian Nordbank this meant autonomous operations, real-time visibility and AI-driven remediation running entirely inside the sovereign perimeter, with no telemetry leaving the jurisdiction. Automated FinOps analysis surfaced idle and over-provisioned capacity continuously, which is where a material share of the run-rate saving came from.

“We did not want a cloud that promised sovereignty in a contract clause. We wanted one where we held the keys, we held the logs, and we could show a supervisor exactly who could touch what. That is what we got — and we got the GPU capacity our data science team had been waiting a year for.”

Group Chief Information Officer, Meridian Nordbank

THE RESULTS

Outcomes after twelve months

MEASURE	BEFORE	AFTER
Workloads under sovereign control	Core banking only	1,400+ across core, analytics and AI
Encryption key custody	Provider-managed	Bank-owned and in-jurisdiction
Mean time to resolution	Baseline	63% lower via AIOps remediation
Infrastructure run-rate	Baseline	31% lower
AI model training	Blocked 11 months	In production on in-perimeter GPUs
DORA exit-plan evidence	Not demonstrable	Documented and supervisor-accepted
Platform availability	Multi-provider, variable	99.999% SLA, single accountable provider

GET STARTED

Cloud That Belongs to You, Wherever You Operate

If your organisation cannot compromise on where its data lives, who can access it, or which laws govern it, UPC Sovereign Cloud was built for exactly that. Talk to our team about a sovereign architecture mapped to your jurisdiction and your regulators.

EMAIL

contact@unitedlayer.com

CALL

+1-888-853-7733

Why UnitedLayer

25+ years of private cloud expertise across 175+ locations on five continents, with follow-the-sun engineering teams providing end-to-end platform management and proactive lifecycle support. Recognised as a Leader in the ISG Private/Hybrid Cloud – Data Centre Services study for four consecutive years.

Available worldwide. Technical support is available 24/7. Custom pricing and demonstrations on request.

UPC Sovereign Cloud is part of the United Private Cloud® portfolio, alongside UPC IaaS, UPC Container Cloud, UPC AI Factory, UPC DRaaS, UPC Cyber Vault, UnitedEdge®, UnitedConnect® and UnitedSecure™.

This case study describes a representative customer scenario constructed to illustrate UPC Sovereign Cloud capabilities. Customer name and figures are illustrative and should be replaced with verified references before external publication.