CUSTOMER SUCCESS STORY

DORA-ready infrastructure, without a migration scramble.

A European bank faced overlapping obligations — DORA, GDPR — that reached past application hosting into operational resilience and third-party control. **UPC Sovereign** gave it an estate designed around those requirements rather than retrofitted to them.

Three regimes — **Compliance had widened beyond where applications run.** The bank had to demonstrate control over data location, identity, key custody, administrative operations, auditability, backup and recovery, incident response, and personnel access — across three overlapping regulatory regimes at once.

THE SITUATION

Obligations that reached into operations

The bank's existing cloud footprint satisfied data-location rules and very little else. Each supervisory conversation surfaced the same gaps:

- **Third-party concentration risk.** Critical workloads sat with a provider whose operational model the bank could neither inspect nor constrain.
- **Recovery crossed jurisdictions.** Disaster-recovery copies replicated to regions outside the supervisory perimeter.
- **Privileged access was opaque.** The bank could not evidence who administered its environment, from where, or under what approval.
- **Evidence was assembled manually.** Each audit cycle consumed weeks reconciling logs across provider consoles and internal systems.

THE DECISION

Design for the regulation, not around it

The bank moved regulated workloads onto a dedicated environment natively aligned with GDPR and DORA, with continuous compliance monitoring built into the platform rather than bolted on.

> *"Our supervisor does not ask where the application runs. They ask who could access it, what happens when it fails, and how I know. Those are operational questions, and they needed an operational answer.*
>
> — CHIEF INFORMATION SECURITY OFFICER

DEPLOYMENT SNAPSHOT

SECTOR	**European banking group**
WORKLOADS	**Core banking · Payments · Risk & reporting**
EDITION	**UPC Sovereign Core**
ALIGNMENT	**GDPR · DORA**
TENANCY	**Dedicated, single-tenant, strictly isolated**
RESILIENCE	**Native Backup and DRaaS in-jurisdiction**
GOVERNANCE	**Policy-as-code with real-time audit visibility**
OPERATIONS	**Fully managed, follow-the-sun support**

WHAT SITS INSIDE THE BOUNDARY

Data	Core banking, payments, and reporting data with **backups and DR copies** retained inside the supervisory perimeter.
Resilience	Native Backup and **Disaster Recovery as a Service** with built-in cyber resilience, designed so recovery never breaches residency.
Governance	**Policy-as-code** governance with centralized control and real-time audit visibility across the estate.
Compliance	Continuous compliance monitoring through **automated AIOps and FinOps**, with a dedicated advisory team tracking regulatory change.

WHAT CHANGED

BEFORE UPC SOVEREIGN

- DR copies replicating **outside** the supervisory perimeter
- Provider operating model neither inspectable nor constrained
- Privileged access impossible to evidence
- Audit evidence assembled **manually** each cycle
- Compliance posture known only at audit time

WITH UPC SOVEREIGN

- Recovery designed to **preserve sovereignty**
- Dedicated, single-tenant estate under bank governance
- Administrative access restricted and recorded
- Policy-as-code with **real-time** audit visibility
- Continuous compliance rather than point-in-time

WHERE THE ASSURANCE CAME FROM

Resilience inside the perimeter

Backup and DR were designed so that recovery — the moment sovereignty is most likely to break — keeps every copy inside the required boundary.

Native regulatory alignment

Aligning to GDPR and DORA at platform level meant the bank inherited controls rather than implementing each one itself.

Continuous, not periodic

Automated compliance monitoring turned audit preparation from a recurring project into a reporting exercise against live data.

WHY THIS MATTERS IN FINANCIAL SERVICES

Controls and frameworks doing the work in this deployment:

DORA operational resilience · GDPR residency · Third-party risk control · Sovereign DR · Policy-as-code governance · Real-time audit visibility

BOTTOM LINE

UPC Sovereign gave a European bank an estate built to the regulation — resilient, inspectable, and provably in-jurisdiction.

Build your sovereign cloud strategy with UPC.

Speak with a specialist, or ask us to map your residency and jurisdictional requirements.

UPC SOVEREIGN™
UNITEDLAYER.COM

EMAIL contact@unitedlayer.com
PHONE +1-888-853-7733
X x.com/unitedlayer
LINKEDIN linkedin.com/company/unitedlay

Customer anonymised at their request; the profile and quotation shown are representative of a European banking deployment. Outcomes described are qualitative and reflect the control and governance changes UPC Sovereign enables; they are not measured benchmarks, and results vary by jurisdiction, edition, and configuration. Certifications and regulatory alignments vary by region and should be confirmed for your requirements. UnitedLayer®, United Private Cloud®, and UPC Sovereign™ are marks of UnitedLayer.

© 2026 UNITEDLAYER. ALL RIGHTS RESERVED.