UPC SOVEREIGN™

UNITEDLAYER®

CLOUD THAT BELONGS TO YOU, WHEREVER YOU OPERATE

Cloud you control.
Data that stays yours.

Secure, high-performance cloud infrastructure for **government agencies, enterprises, and regulated industries** that require data residency, sovereignty, and operational independence.

Reside **Govern** **Prove** **Operate**

THE CHALLENGE

Cloud adoption should not mean losing control

Cloud delivered speed, scale, and flexibility. For regulated and mission-critical organisations it also introduced a set of questions that a standard public-cloud region cannot always answer.

Questions your auditors, regulators, and customers will ask:

- Where is your data stored, and where is it processed?
- Who can access it — and from which country?
- Where do backups, logs, and metadata reside?
- Does support or incident response cross borders?
- Which legal jurisdiction actually governs it?
- Who owns and operates the underlying infrastructure?
- Who controls the encryption keys?
- Can you prove all of this to an auditor?

WHY IT IS HARDER THAN IT LOOKS

A local region is not sovereignty

A data centre in-country does not by itself settle jurisdiction, infrastructure ownership, where administrators sit, who holds keys, or whether support crosses borders.

Secondary data leaks the boundary

Primary data may stay in region while backups, snapshots, metadata, logs, and support access move elsewhere — leaving real residency and compliance exposure.

Control is hard to prove

Privileged access, key custody, data movement, and operational process often rest on provider assurance rather than evidence the customer can inspect.

Compliance has widened

Obligations now reach identity, key custody, administrative operations, auditability, backup and recovery, incident response, and personnel access — not just where an app runs.

THE GAP

For sensitive workloads, "secure by design" is no longer enough. Control has to be demonstrable.

THE SOLUTION

A sovereign cloud built around control

UPC Sovereign is a dedicated private cloud for enterprises and government bodies that cannot compromise on where their data lives, who can access it, or which laws govern it. Every layer — **compute, storage, network, and security** — is provisioned exclusively for you, within your chosen sovereign boundary.

Data sovereignty

Your data is subject to the laws of the country where it is stored, and only those laws. No hyperscaler access. No cross-border replication without consent.

Operational sovereignty

Always-on, always-in-jurisdiction. Critical applications stay resilient even during regional disruption, with business continuity and disaster recovery built in.

Digital sovereignty

You own and control the encryption keys, the access policies, and the audit trail — with full transparency and policy-as-code governance under centralized control.

BUILT FOR NEXT-GEN WORKLOADS AND LEGACY COEXISTENCE

Dedicated sovereign architecture

Dedicated, single-tenant private clouds engineered for strict isolation, using residency-specific access controls that restrict data management exclusively to authorized regional personnel.

Compliance & governance

Natively aligned with GDPR, DORA, NIS2, and BSI C5, with automated AIOps and FinOps for continuous compliance, deep observability, and cost optimization.

Native backup

Fully integrated Backup and Disaster Recovery as a Service, with built-in cyber resilience to mitigate evolving security threats.

Fully managed operations

End-to-end cloud platform management and proactive lifecycle support, delivered across a global presence via follow-the-sun engineering teams.

25+
Years of private cloud expertise

175+
Delivery locations, five continents

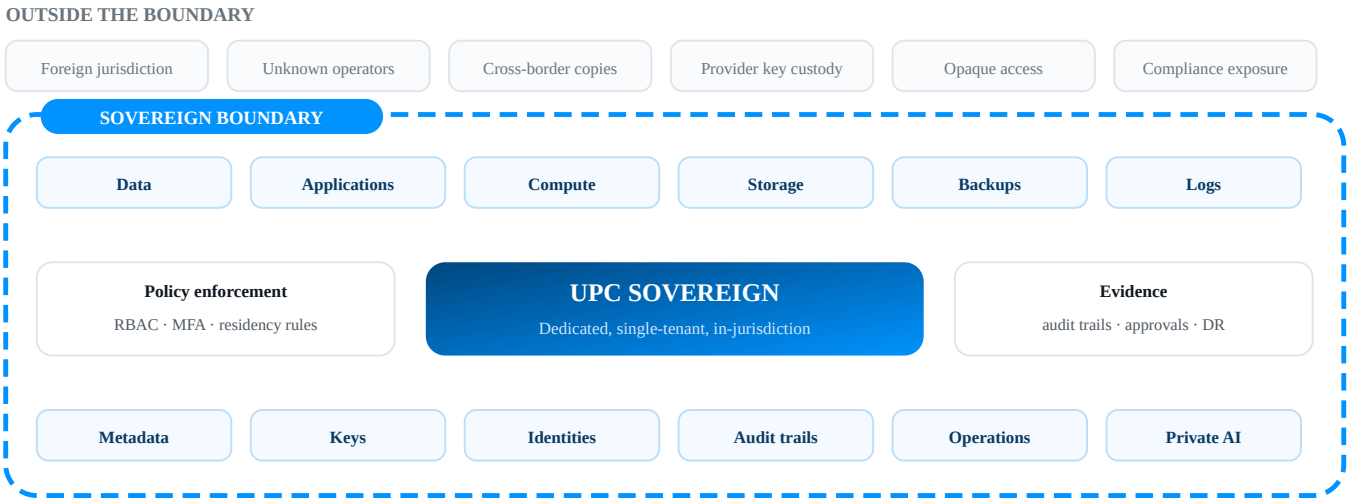
15+
Global compliance frameworks

99.999%
Availability SLA

HOW IT WORKS

Everything important stays inside a controlled territory

Sovereignty fails at the edges — in the backup that replicates abroad, the log shipped to a central service, the administrator connecting from another jurisdiction. The design principle is simple: every artefact that carries your data follows the same residency rule as the data itself.



Everything that matters stays inside a controlled digital territory.

FIGURE — THE SOVEREIGN BOUNDARY

THE RESIDENCY RULE, APPLIED

ARTEFACT	COMMON EXPOSURE IN A STANDARD CLOUD REGION	UNDER UPC SOVEREIGN
Primary data	Usually in-region	In-region, governed by that jurisdiction alone
Backups & snapshots	May replicate to another region by default	Retained inside the sovereign boundary
Logs & metadata	Often shipped to centralized provider services	Stored and monitored in-boundary
Encryption keys	Frequently provider-managed	Customer-owned and customer-controlled
Administrators	May be global follow-the-sun staff	Restricted to authorized regional personnel
Support & incident response	May cross borders during escalation	Governed by policy, with break-glass on customer approval

CORE CAPABILITIES

Control, expressed as platform capability

Sovereign data residency
Keep data, backups, logs, metadata, and processing within a defined geographic or regulatory boundary.

Jurisdictional control
Align data and infrastructure operations with the laws and governance requirements of the designated jurisdiction.

Dedicated private infrastructure
Run critical workloads on secure, single-tenant infrastructure engineered for strict isolation and enterprise performance.

Privileged-access governance
Restrict administration by role, residency, approval, time, and business need, with mandatory strong authentication.

Customer-controlled encryption
You own and control the master encryption keys, separating infrastructure administration from data decryption.

Auditable operations
Real-time access logging and tamper-evident audit trails, retained inside the sovereign boundary.

Break-glass control
Emergency access follows documented procedures requiring customer approval and producing an auditable record.

Secure private AI
Run models, agents, RAG pipelines, and sensitive inference inside the boundary, with enforceable identity and execution limits.

Resilience in-jurisdiction
High availability, backup, and disaster recovery designed so recovery copies never leave the required boundary.

PRE-CERTIFIED ACROSS GLOBAL FRAMEWORKS

GDPR · DORA · NIS2 · BSI C5 · KRITIS · ISO 27001 · ISO 27017 · ISO 27018 · ISO 14001 · SOC 1 / SOC 2 · PCI DSS · HIPAA · FedRAMP · FISMA · NIST · FINRA · ITAR · CJIS · FIPS · SSAE · AICPA

A dedicated compliance advisory team tracks regulatory change across jurisdictions, so your teams do not have to.

WHAT'S INCLUDED

Purpose-built for every sovereign workload

UPC Sovereign ships with a native intelligence layer — **Unified Observability, AIOps, and Agentic Orchestration** — built directly into the platform, so autonomous operations, real-time visibility, and AI-driven remediation all run inside your sovereign perimeter.

UPC Sovereign Core

- Fully managed private cloud at your sovereign-chosen location
- Compliance-aligned with GDPR, DORA, NIS2, BSI C5 and others
- Multi-hypervisor support: VMware, KVM, Hyper-V, Canonical
- Built-in Observability, AIOps, and Agentic Orchestration

UPC Secure Multi-Cloud Orchestration

- Data sovereignty and policy enforcement across multiple clouds
- Centralized policy-as-code governance with real-time audit visibility
- AI-driven automation for workload placement and compliance
- Single control plane for public cloud, private cloud, and edge

UPC AI-Optimized Sovereign Cloud

- Dedicated GPU clusters within your sovereign perimeter
- Data processing pipelines for AI model training and inference
- End-to-end data encryption in transit and during model training
- EU AI Act compliance mapping and data lineage documentation

UPC High Performance Computing Sovereign

- Optimized virtual infrastructure for compute-intensive workloads
- High-throughput interconnects within the sovereign boundary
- Scalable architecture with dedicated storage tiers
- Certified for national security and critical infrastructure

PART OF THE PORTFOLIO

UPC Sovereign sits within the United Private Cloud® suite, alongside UPC AI Factory, UPC Vektor, UPC Container Cloud, UPC DRaaS, and UPC Cyber vault.

USE CASES

Where sovereignty is not optional

Government & public sector

Citizen data, administrative systems, and public-service workloads hosted in-country with controlled administrator access and protected backups and logs.

Financial services

Segregated infrastructure, strong privileged-access policy, audit-ready operations, and secure AI for fraud detection, risk, and customer operations.

Healthcare & life sciences

Protected health data, controlled processing, private analytics and AI, and resilient clinical applications with auditable administrative access.

Critical infrastructure

Operational technology data, infrastructure telemetry, security events, and industrial applications with strict operational control and sovereign DR.

Sensitive intellectual property

Product designs, source code, research data, and proprietary models on dedicated infrastructure with customer-controlled keys and restricted admin access.

Regulated service providers

Localized cloud offerings, tenant-level isolation, sovereign backup and recovery, and managed private AI for sector-specific services.

BENEFITS BY STAKEHOLDER

STAKEHOLDER	CHALLENGE	UPC SOVEREIGN BENEFIT
CIO	Cloud adoption creates strategic and regulatory risk	Cloud agility with stronger control over data, operations, and jurisdiction
CISO	Provider access and data movement are hard to govern	Identity, residency, MFA, key, logging, and privileged-access controls
Compliance	Residency and operational compliance are hard to prove	Clearer evidence through controlled architecture and auditable operations
Government leader	Public data and services require sovereign protection	Citizen and government workloads hosted within a controlled boundary
Infrastructure	Sensitive workloads need performance and isolation	Dedicated, single-tenant infrastructure for critical applications
Data & AI teams	AI requires sensitive enterprise data	Private AI and model workloads inside a governed perimeter
Business leadership	Security controls can slow transformation	Modernize with cloud capability without giving up sovereignty

HOW IT DIFFERS

Sovereign cloud versus standard public cloud

DIMENSION	STANDARD PUBLIC CLOUD	UPC SOVEREIGN
Data location	Region-selectable, but with broader service dependencies	Designed around a defined sovereign boundary
Backups & metadata	May be distributed across provider services and regions	Designed to remain within the required boundary
Administrator access	Provider access may be global or hard to constrain	Restricted to authorized regional personnel by policy
Encryption keys	Often provider-managed by default	Customer-owned and customer-controlled
Jurisdiction	May carry foreign legal exposure	Aligned to the designated jurisdiction, and only those laws
Infrastructure	Shared or provider-standard	Dedicated, single-tenant, strictly isolated
Compliance evidence	Depends on provider certifications and contracts	Supported by access controls, logs, policy-as-code, and architecture
AI workloads	May require data movement to external services	Dedicated GPU clusters inside the sovereign perimeter
Resilience	May span multiple regions or jurisdictions	Backup and DR designed to preserve sovereignty

BOTTOM LINE

Modernize with confidence. Operate with control. The power of cloud, with sovereignty built in.

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