OPCP

On-Prem Cloud Platform

Stability. Sovereignty. Performance.

A next-generation, high-performing cloud solution, built for scale and operated to meet sovereignty requirements and optimise performance.

OPCP
by OVHcloud

The core functions of government: institutions, which uphold, defend, and reshape public authority.

National governments, along with their respective ministries, public bodies, and agencies, are the **foundational pillars that enable public governance throughout Europe.**

They are responsible for designing, coordinating, and implementing public policies that fundamentally shape societies and support national progress.

In fields such as public finance, health, justice, security, ecological transition, critical infrastructures, as well as innovation and research, these institutions play a key role in essential, often linked, areas **where reliable government action is decisive.**

Their duties encompass everything from strategic planning to practical implementation, all with the shared goal of ensuring institutional stability, the uninterrupted and effective delivery of public services, and the safety of citizens.

As a result, these institutions manage day-to-day operation such as:

- → **complex administrative processes,**
- → **massive volumes of data,**
- → **essential services requiring consistent uptime,**
- → **critical operations requiring a high level of security and reliability,**
- → **national and European-level coordination involving various sites and providers.**

Beyond their institutional duties, they **directly contribute to economic success.** A country becomes more attractive when it is modern, stable, and digitally advanced, promoting innovation, operational efficiency, and trust among domestic and international businesses.

As a result, effective and efficient institutions are crucial for the success of a modern and prosperous society.

Advancements in technology create new possibilities for government action.

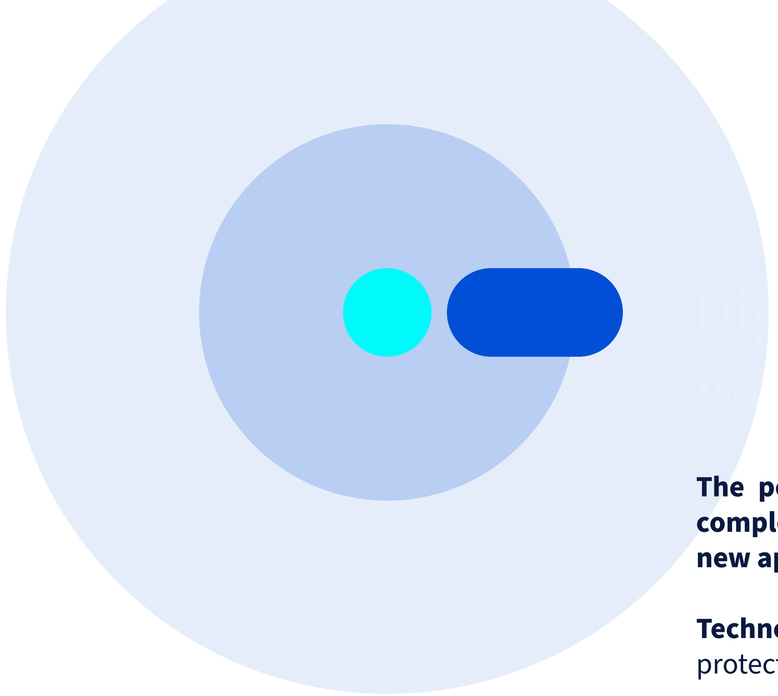
Public sector bodies are operating in a rapidly changing technological environment. **The rise and maturity of new technologies**, such as cloud computing, automation, massive data processing, and distributed platforms, provide new avenues for the planning and rollout of government initiatives.

Thanks to these technologies, **public services** can now be designed to be **more agile,** capable of adapting quickly to new regulations, citizens' expectations, and crises. They enable the deployment of on-demand public services, the automation of complex processes, large-scale data utilisation, and improved capacity to guide public policies.

They also change how government services operate by closely aligning digital tools with operational requirements. Responsibilities are shared between central operations and front-line services — with a strong focus on local implementation — creating opportunities for greater efficiency, resilience, and foresight.

However, fully capitalising on these new technologies is unachievable without **the right underlying infrastructure.** The potential of modern technologies will remain largely out of reach, if not completely inaccessible, without the necessary infrastructure to support these new use cases.

This gap between the possibilities offered by current technologies and the reality of public infrastructures makes digital modernisation essential.



The potential of modern technologies will remain largely out of reach, if not completely inaccessible, without the necessary infrastructure to support these new applications within government services.

Technological innovation cannot be divorced from sovereignty, security, and data protection requirements.

Government bodies and agencies handle sensitive data concerning citizens, businesses, and national strategic interests. They are required to do this within environments that ensure data control, access traceability, and regulatory compliance, and while providing the government with robust control over its digital assets.

Here, sovereignty acts not as a barrier to innovation but as a foundation for its longterm viability. It enables public institutions to adopt the most advanced technologies (cloud computing and AI), while ensuring data security, proper management of technological dependencies, system reversibility, and well-managed updates.

This ability to scale, innovate, and transform — all while protecting the data of citizens and national businesses — underpins responsible long-term digital modernisation of public services.

Digital sovereignty as a driver of competitiveness, security, and influence.

Today, a nation's digital sovereignty is as vital as data protection and infrastructure management to its economic competitiveness and global influence.

Technologies, data, and digital platforms have a direct impact on the resilience of national industries and the trust of businesses.

They can innovate, invest, and grow within a sovereign digital environment thanks to stability, security, and predictability.

By protecting strategic know-how and minimising critical technological dependencies, this sovereignty promotes the growth of competitive industrial ecosystems that can compete in European and global markets.

Digital sovereignty enhances the security of public services. It ensures that sensitive personal data, essential services, and critical infrastructure operate under strict guidelines, thereby lowering the chances of tampering, unauthorised access, or external interference.

In fact, it is a key lever for exerting influence in international affairs. When a country can independently shape its digital infrastructure, secure its essential systems, and regulate its data flows — it strengthens its standing, bargaining power, and strategic autonomy in a highly networked world.

Protection is no longer the sole focus of digital sovereignty, **but rather a pillar of competitiveness, collective security, and long-term standing on the global stage.**

Strengthening government initiatives through digital advancements.

To keep up with long-term government initiatives, integrating new technologies requires going beyond just the initial digital deployments.

Having already benefitted from its shift to digital, paperless processes, European countries are now entering a new phase of their transformation. The shift is from merely digitising existing workflows to a thorough overhaul of the foundations of public service delivery.

With the rise of digital usage, extensive data mining, and the integration of advanced technologies such as AI, a significant overhaul is required in how organisations are structured, operate, and are technologically equipped.

This involves changing how governments and their agencies operate to fully utilise digital technologies, without compromising consistency, oversight, and continuity.

A new era is emerging, marked by well-defined projects that fundamentally transform how the government plans and delivers public services.

Turning sovereign technological potential into lasting operational capabilities.

New technologies offer public institutions new possibilities, but adopting them is not simply about layering on additional tools. To create real impact on public services, these capabilities have to be incorporated into well-organised, controlled environments that meet institutional demands.

The government's transformation projects are now required to **turn technological potential into real-world operational strengths, including:**

- → rapid deployment of new services,
- → reliable automation and industrialisation of operations,
- → secure data mining,
- → uninterrupted services even during emergencies
- → the capability to adapt to a wide range of
- → operational scenarios, at the edge or in critical airgapped setups.

It involves making digital technologies more accessible and relevant to realities on the ground, while supporting a unified national strategy.

Reaping lasting benefits from new technologies is difficult without an adequate underlying technology. Infrastructures should be able to support these uses over time, evolve without disruption, and guarantee a high level of security, resilience, and oversight.

Currently, the key to modernising public services depends on how well digital systems are structured, maintained, and regulated.

Central governments faced with increasing digital and operational challenges.

With growing digital use and demanding public expectations, central government services and national agencies face increasingly complex IT systems.

They must deliver crucial activities, handle large amounts of sensitive data, and support government transformation projects. All while ensuring performance, continuity, and digital sovereignty are maintained.

Information systems operate under significant limitations.

Ministries, general directorates, agencies, and state-run organisations still rely heavily on outdated, heterogeneous, and highly interdependent systems. This fragmented setup makes it harder to modernise applications, burdens daily operations, and increases risks for applications that are often crucial for public services.

When oversight responsibilities are spread across various entities, this leads to overlapping functions, uneven digital maturity, and significant strain on information systems. This is particularly challenging given the constant need for enhanced, rapid, and uninterrupted public services amid reforms, regulatory shifts, or crises.

A growing reliance on digital tools and technologies.

At the same time, the government as well as its services and agencies are becoming more and more data-driven. The rapid growth of public data (across social, fiscal, environmental, health and mobility sectors), along with the widespread adoption of remote services and online processes, and the rise of AI, analytics and predictive demands, is placing increasing pressure on their infrastructure.

This ongoing trend highlights the need **for genuine interoperability between government bodies and state-run organisations,** which in turn puts a burden on infrastructures and organisations that struggle to adapt to these emerging uses.

Structural issues in national modernisation projects.

Central government services and agencies are now undergoing digital transformation, driven by these key factors:

- **Sovereignty and trust**, through total control of data, flows, and access policies,
- **Security and resilience** to ensure the continuity of essential services,
- **Phased modernisation**, to update and scale critical systems without disruption,
- **Streamlined processes and cost control**, with limited resources and improved budgeting,
- **Interoperability and innovation** to drive the creation of shared services, advanced data mining, automation, and the regulated use of AI.

Due to these challenges, central governments are required to redesign their digital infrastructure to make it more durable, ensuring the efficiency of public services and strengthening national sovereignty.

Next-gen cloud infrastructures provide the foundation for public services.

Modernising public services through new technologies requires more than just the public cloud or legacy systems.

To meet the real needs of current and future administrations, the government must rely on **state of-the-art infrastructures**, capable of operating:

- → **to support central governments** (ministries and national platforms),
- → **at the edge** (remote sites, prefectures, laboratories, executive agencies),
- → **in sensitive environments**(restricted access areas, specialised networks, classified spaces),
- → **in offline mode** (crisis, network outage, field operations).

These new use cases demand an infrastructure that can:

- → **deploy** applications, environments or services in minutes,
- → **operate locally**, even with an unreliable network-connection,
- → **be fully automated,**
- → **adapt to diverse workloads,**
- → **protect the most sensitive data,**
- → **ensure very low latency for edge computing,**
- → **completely isolate certain processes (airgapped),**
- → **integrate seamlessly with public cloud setups when relevant,** without dependency.

Simply put, national digital reach must reflect three overlapping strategies:

- → **The cloud:** elasticity and scalability.
- → **Modernised on-prem setup:** control, sovereignty, and continuity.
- → **Edge and air-gapped environments:** operational proximity, security, and autonomy.

OPCP: a next-generation on-prem platform to meet all your needs.

OPCP is more than a basic local cloud; it is **a cloud-native platform that can be installed within government infrastructures, particularly:**

- → **in a ministry's datacentre,**
- → **on a critical site,**
- → **in a prefecture or an executive agency,**
- → **in an isolated setup,**
- → **in disconnected mode,**
- → **or as an addition to a public cloud setup.**

OPCP provides the government with a local infrastructure as modern as the cloud, with:

- → **automated deployment on demand,**
- → **ready-to-use service catalogue,**
- → **instant provisioning,**
- → **standardisation between departments,**
- → **hardened security,**
- → **centralised governance and fine-grained segmentation,**
- → **simplified operations,**
- → **autonomous operation in all configurations (edge computing, air-gapped mode, remote, crisis)**

A comprehensive solution designed to meet the diverse needs of government:

- → For a ministry: **to seamlessly modernise IT systems** and support critical workloads.
- → For an agency: **to host sensitive data** with total sovereignty.
- → For an executive agency: **to have local resources**, even without a network connection.
- → For an independent authority: **to completely isolate specific processes.**
- → For sovereignty-oriented duties: to ensure **full resilience and availability.**

With OPCP, state-run cloud infrastructure evolves from a legacy system into a powerful accelerator.

A single architecture designed for all applications, from national datacentres to air-gapped operations.

Government services cannot rely on a single infrastructure; they require **an architecture that can operate seamlessly across diverse environments** and configurations, with extensive automation.

OPCP CORE

An automated and resilient foundation.

- Complete orchestration (compute, network, security)
- Advanced observability
- Automatic updates
- Autonomy in disconnected sites
- Multi-level resilience
- With integrated security hardening

OPCP Core facilitates the deployment of an up-to-date platform, **whether in a ministry or a classified basement.**

LANDING ZONE MANAGER

Fine-grained governance for distributed environments.

- Isolation by ministry, directorate, agency, or state-run organisation
- Custom compliance policies
- Advanced management of roles, quotas, and access
- Suitable for sensitive or restricted environments
- Manageable at the national or local level

It enables **standardised oversight**, all while respecting the functional boundaries of each public entity.

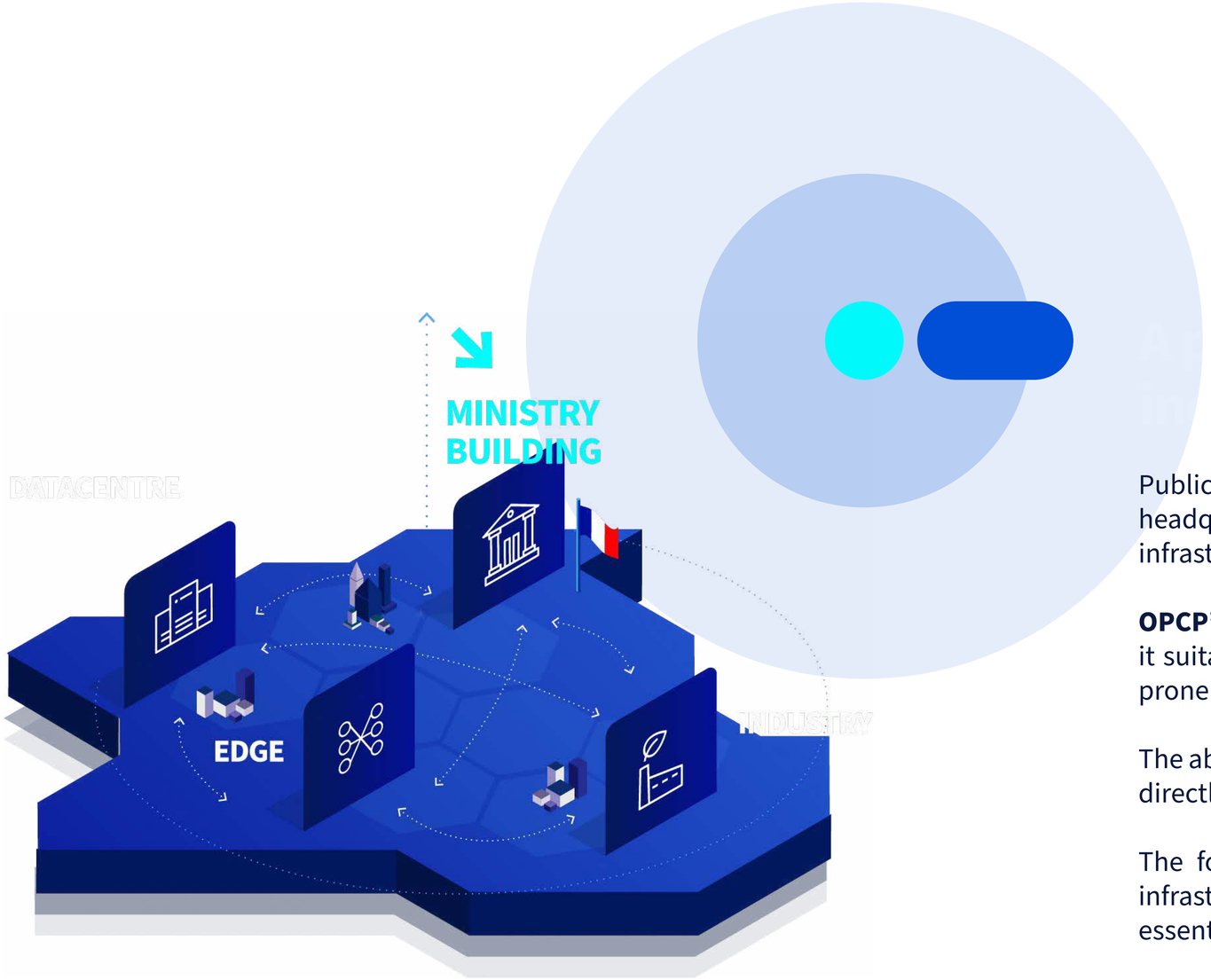
CLOUD STORE

Instant service deployment, including in isolated local environments.

- A catalogue of standardised applications and services
- VMs, databases, AI stacks, analytics services, microservices
- Deployable **at the edge or in air-gapped environments**
- Standardisation across remote centres and sites

With OPCP Cloud Store, public services can be deployed **on-site** in just a few minutes:

- analytics platforms
- business tools
- databases
- AI engines
- critical local services

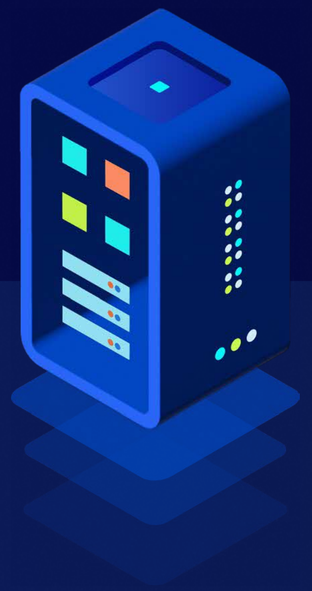


Public institutions **operate across highly diverse environments**, from ministerial headquarters and remote facilities to laboratories, crisis centres, critical infrastructure and sites requiring full isolation.

OPCP's architecture is designed **to handle a wide range of use cases**, making it suitable for environments ranging from secure, isolated systems to networks prone to frequent disruptions.

The ability to adapt is more than just a concept; it translates to practical uses that directly address the needs of ministries, agencies, and state-run organisations.

The following use cases illustrate how OPCP enables the modernisation of infrastructures, strengthens sovereignty, speeds up deployments, and secures essential public services, regardless of operational environments or constraints.



OPCP

USE CASE | **01**

Gradually and securely modernising critical government systems.

Modernising public services without compromising sovereignty.

Governments rely on critical legacy systems, relating to tax systems, national registers, judicial systems, internal security, social security records and market regulation. Due to their design dating back several decades, these systems are difficult to migrate and highly interconnected and, most critically, are required to operate uninterrupted. Hence, any technical updates to these systems must be carefully managed, rolled out gradually, and fully secured.

OPCP ensures:

- → **the phased integration of** modern services without disrupting current systems,
- → **the automation** of routine tasks (patching, security, updates),
- → **the move towards unified technical environments**, reducing discrepancies between entities,
- → **security for critical workloads** while preparing for their modernisation,
- → **smooth continuity** during version updates, migrations, or overhauls.

OPCP supports the ongoing, controlled, and uninterrupted modernisation of sovereign systems, which is crucial for institutional stability.

OPCP

USE CASE | **02**

A sovereign environment for sensitive government data.

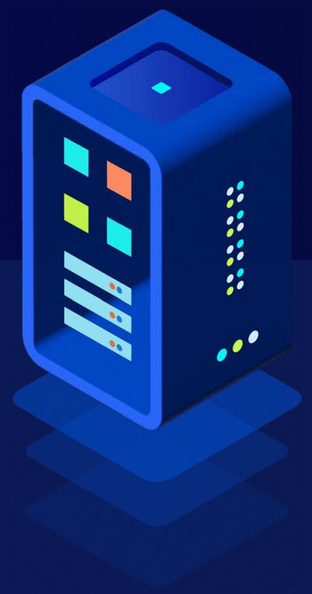
Creating a secure and controlled national data hub.

Public data has become a strategic asset, driving policy-making in areas such as social welfare, environmental protection, conomic growth, public health. However, this data is often distributed across heterogeneous systems, sometimes hosted by third parties, making its governance, analysis, and security more challenging.

OPCP facilitates:

- **the centralisation of sensitive data** in a sovereign, government-owned environment,
- **fine-grained access management** based on data sensitivity and classification levels,
- **secure**, on-site **execution** of analytical or AI processes without external exposure,
- the **standardisation of formats and flows** to facilitate inter-agency sharing,
- the **complete isolation** of critical processes (restricted areas, airgapped environments, classification levels).

Governments can utilise OPCP's sovereign scale to maximise their data's potential, while retaining full control over their flow, security, and integrity.



OPCP

USE CASE | 03

The continuity of national affairs in the ace of crises, cybersecurity issues, and sensitive operations.

Maintaining the continuity of government functions, regardless of circumstances.

Governments must ensure the continuous availability of their systems supporting public safety, payment processing, tax collection, crisis management and interministerial coordination. However, recent crises (cyberattacks, natural disasters, geopolitical tensions) now highlight the need for increased resilience, which can maintain operations even when conditions are less than ideal.

OPCP supports:

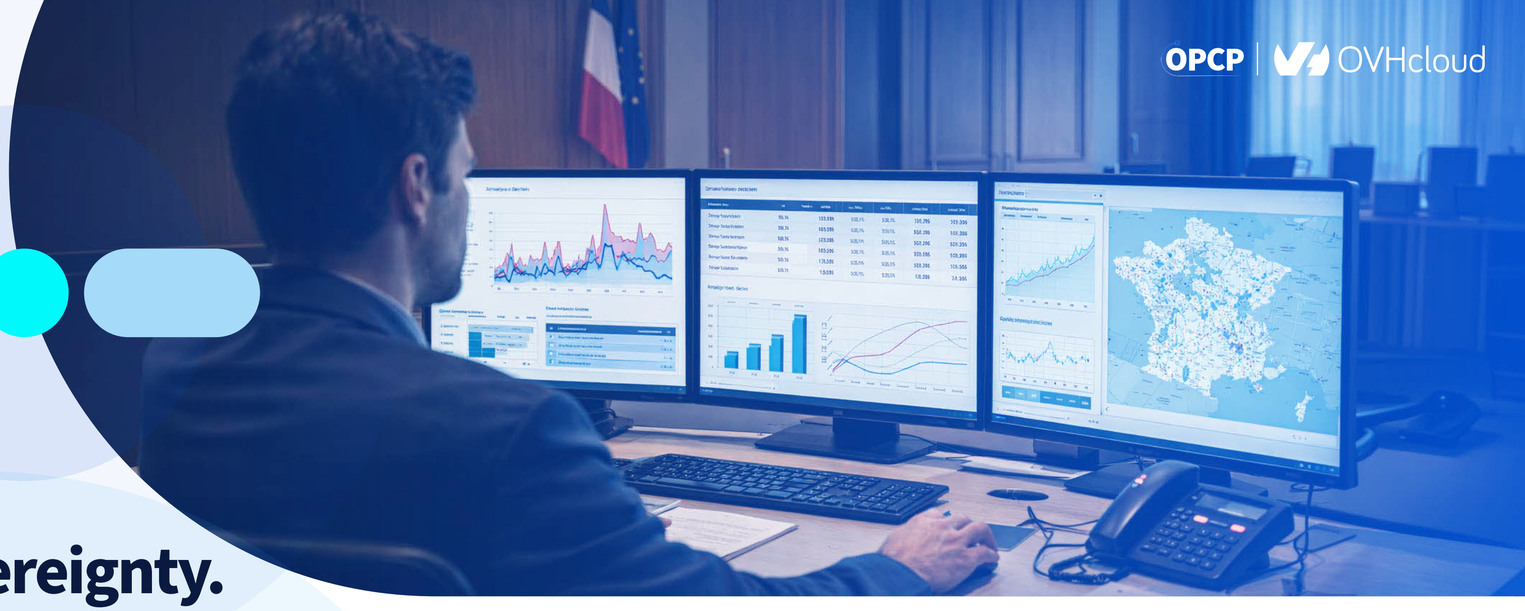
- → the **local delivery** of services, even during network outages, or in complete isolation,
- → the **urgent deployment** of tools to support public services during crises,
- → the **support of tactical or sensitive environments** by utilising secure edge nodes,
- → the **continuity** of essential public services (payment, health, security), even in less than ideal circumstances,
- → **enhanced cyber defence,** built upon a secure and self-dependent infrastructure.

In a world where crises can occur at any time, OPCP ensures the continuous availability of government services.

OPCP

USE CASE | **04**

A national AI platform designed to ensure sovereignty.



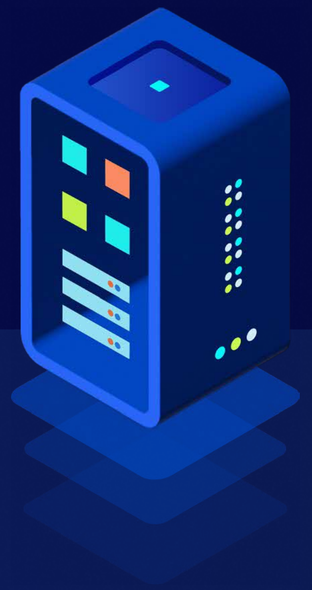
Leveraging AI without exposing sensitive data.

Governments are looking to leverage AI to support policymaking, identify irregularities, process extensive regulatory data, speed up inspections, better serve citizens, and predict potential crises. However, the data required by AI models is sensitive and often classified, meaning it must remain within the nation's borders.

OPCP facilitates :

- → **the hosting of AI models** within a sovereign and secure infrastructure,
- → **the training of models** on sensitive data without it leaving controlled boundaries,
- → **the setup of an air-gapped environment**, especially when maximum isolation is a necessity,
- → **the pooling of GPU resources** or advanced compute capabilities between ministries,
- → **the building of specialised AI models** based on departments: security, tax, justice, environmental protection, or public health.

With OPCP, the government can ensure the sovereign and controlled use of AI, aligned with the protection of the most sensitive data.



OPCP

USE CASE | **05**

A unified platform for shared services between ministries and agencies.

Resource sharing to harmonise, reduce costs, and strengthen government action.

When infrastructure is split across different ministries, agencies, and state-run organisations, it leads to costly overlaps, hard-to-manage duplicate systems, heterogeneous processes and operational overload. Sharing resources is crucial for boosting efficiency and making the best use of public funds.

With OPCP, they can:

- → **unify various government entities on a single infrastructure** while maintaining their distinct organisational structures,
- → **implement uniform standards for** data security, compliance, and governance,
- → **optimise hardware and software resources** through standardisation,
- → **limit dependence** on a wide range of different providers,
- → **support cross-departmental projects** and facilitate cooperation between ministries.

OPCP provides the foundation for modern, national digital resource sharing, enabling governments to improve efficiency, coordination and their capacity to act.

A pairing with purpose

Proven technical solution, combined with industry-specific expertise.
Clearly, there are things we need to do together.

Cases to develop, adapt, and test

There’s no shortage of use cases: edge, factories, critical sites, disconnected infrastructure, and much more. What if we focused on one or two key areas to make real progress?

A workshop, a chat, a POC?

We don’t need to put everything on hold just yet.
Let’s brainstorm, see which ideas make sense, and gradually build.

ovhcloud.com
opcp@ovhcloud.com