hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN



OVHcloud

OVHcloud

System and Organization Controls (SOC 3®) Report

On Security, Availability, Confidentiality and Privacy

Covering the Public Cloud System of OVHcloud

For the Period from January 1, 2025 to December 31, 2025

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Table of content

SECTION I Independent Service Auditor's Report 4
SECTION II Management of OVHcloud's Assertion 8
SECTION III Attachments 10
Attachment 1 - OVH Groupe S.A.'s Overview of Services and the System 11
1. Company Overview and Services Provided 11
1.1. A Vertically Integrated Model, Based on Exclusive Technology 11
1.1.1. A Server and Data Center Integrated Model 11
1.2. OVHcloud Universe of Cloud Offerings 12
1.3. Scope Covered in this Report 17
2. Components of the System Used to Provide the Services 21
2.1. Infrastructure 21
2.2. Software 25
2.3. People 27
2.4. Procedures 29
2.5. Data 31
Attachment 2 - Principal Service Commitments and System Requirements 32
Attachment 3 - OVH Groupe S.A.'s Complementary User Entity Controls 33

Final Version

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

-Intentionally left blank-

Final Version
hf195743ovh

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

SECTION I
Independent Service Auditor's Report

Final Version

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

KPMG

KPMG S.A.
Tour EQHO
2 Avenue Gambetta
CS 60055
92066 Paris La Défense Cedex

To the Board of Directors of

OVH Groupe S.A., Roubaix, France

-hereinafter also referred to as “OVHcloud“ or “the Company“-

Scope

We have examined management of OVH Groupe S.A.’s accompanying assertion titled "Management of OVHCloud’s Assertion" (the Assertion) that the controls within OVH Groupe S.A.'s Public Cloud system (the System) were suitably designed and operating effectively throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Management of OVH Groupe S.A.’s Attachment 3 - OVH Groupe S.A.*’s Complementary User Entity Controls (Attachment 3)* indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.’s service commitments and system requirements based on the applicable trust services criteria. Management of OVH Groupe S.A.’s Attachment 3 presents the complementary user entity controls assumed in the design of OVH Groupe S.A.’s System. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

OVH Groupe S.A. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that OVH Groupe S.A.’s service commitments and system requirements were achieved. Management of OVH Groupe S.A. has provided the accompanying Assertion about the suitability of the design and operating effectiveness of controls within the System. OVH Groupe S.A. is also responsible for preparing the Assertion, including the completeness, accuracy, and method of presentation of the Assertion; providing the services covered by the Assertion; selecting, and identifying in the Assertion, the applicable trust services criteria; identifying the risks that threaten the achievement of OVH Groupe S.A.’s service commitments and system requirements; and having a reasonable basis for the Assertion by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

KPMG S.A., société d’expertise comptable et de commissaires aux comptes inscrite au Tableau de l’Ordre des experts comptables de Paris sous le n° 143008010101 et rattachée à la Compagnie régionale des commissaires aux comptes de Versailles et du Centre.
Société française membre du réseau KPMG constitué de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (private company limited by guarantee).

Société anonyme à conseil d’administration
Siège social :
Tour EQHO
2 avenue Gambetta
CS 60055
92066 Paris La Défense Cedex
Capital social : 5 497 100 €
775 726 417 RCS Nanterre

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on the Assertion that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the Assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the System and OVH Groupe S.A.'s service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria
- performing procedures to obtain evidence about whether controls within the System were suitably designed to provide reasonable assurance that OVH Groupe S.A. would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- testing the operating effectiveness of controls within the System to provide reasonable assurance that OVH Groupe S.A. achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with the relevant ethical requirements in the United States of America relating to the examination engagement. We have complied with those requirements. We have also applied the statements on quality management standards established by the American Institute of Certified Public Accountants and International Standard on Quality Management 1, which require the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, the Assertion that the controls within OVH Groupe S.A.'s System were suitably designed and operating effectively throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system

requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Paris,

August 05, 2026

KPMG S.A.



Xavier Niffle
Partner, Audit



Fayçal El Belghami
Partner, IT

hf195743ovh
Final version

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

SECTION II
Management of OVHcloud's Assertion

Final Version

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Management of OVH Groupe S.A.'s Assertion,

We are responsible for designing, implementing, operating, and maintaining effective controls within OVH Groupe S.A.'s Public Cloud system (the System) throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the System is presented in our Attachment 1 - *OVH Groupe S.A.'s Overview of Services and the System (Attachment 1)* and identifies the aspects of the System covered by the Assertion.

Our Attachment 3 - OVH Groupe S.A.*'s Complementary User Entity Controls (Attachment 3)* indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria. Our Attachment *3* presents the complementary user entity controls assumed in the design of OVH Groupe S.A.'s System.

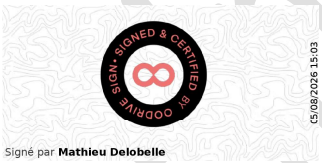
We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria. OVH Groupe S.A.'s objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in our Attachment 2 - *OVH Groupe S.A.'s Principal Service Commitments and System Requirements (Attachment 2)*.

We assert that the controls within the System were suitably designed and operating effectively throughout the period January 1, 2025 to December 31, 2025 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

OVH Groupe S.A

Mathieu Delobelle

Chief Information Officer



August 05, 2026

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

SECTION III
Attachments

Final Version

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Attachment 1 - OVH Groupe S.A.'s Overview of Services and the System

1. Company Overview and Services Provided

OVH Groupe S.A ("OVHcloud") was founded in 1999 as an internet hosting company in France. Over the last 20 years, OVHcloud has developed its infrastructure and expanded its presence in Europe, North America and Asia, diversifying its cloud offerings and expanding its activities globally.

OVHcloud is a cloud provider supported by a vertically integrated production model that provides enterprises with a comprehensive suite of solutions for multi-cloud and hybrid cloud strategies distributed into four core cloud categories:

- **Bare Metal Cloud:** with dedicated physical servers to customers;
- **Hosted Private Cloud:** in a fully dedicated environment to its business customers;
- **Public Cloud:** based on open-source technologies such as OpenStack and Kubernetes;
- **Web Cloud:** with website hosting and domain registration, telecommunications, and internet access.

1.1. A Vertically Integrated Model, Based on Exclusive Technology

1.1.1.A Server and Data Center Integrated Model

OVHcloud has developed an integrated model to fully manage in-house each step of both server and data center lifecycles limiting the dependency on subservice organizations.

OVHcloud's vertically integrated supply chain includes server manufacturing, data center operations, network provisioning and IT infrastructure management. By designing and assembling all its servers in-house, OVHcloud fully owns server design, production and management. OVHcloud has built its strong vertical integration through proprietary technology and in-house operations in various geographies.

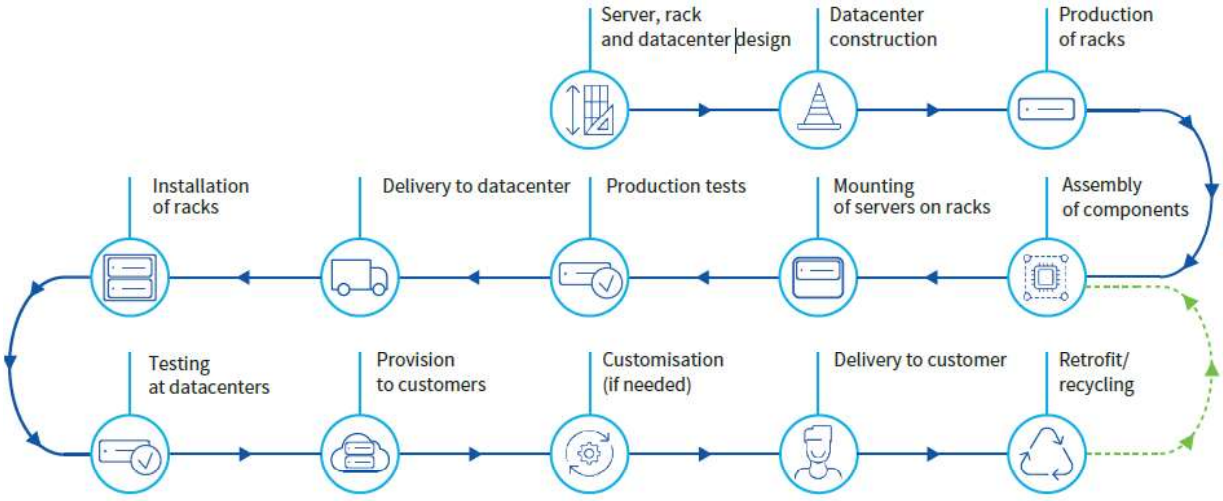


Figure 1: Integrated model for server and data center lifecycle

OVHcloud has two dedicated production sites—in France and in Canada—for assembling different hardware components into servers. Once the various components have been assembled, they are transported to the data center and customized as necessary prior to delivery to the customer.

Inspection Version

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

OVHcloud reduces the risk of supply chain disruption by manufacturing its servers in-house and removing dependencies on a third-party manufacturer.

The capacity to manufacture servers proved to be essential in allowing OVHcloud to respond rapidly to restore service in case of incidents.

1.1.2. A Data Center Proprietary Water-Cooling Technology

OVHcloud has developed and used over 20 years a proprietary water-cooling technology within its data centers. OVHcloud's water cooling technology combines water-cooled servers with air-cooled data centers, thereby removing the need for air conditioning. It uses direct water cooling to remove the heat from CPUs, and air—which is then cooled inside the rack using water through a heat exchanger—to remove the heat from other components. The heated water is then cooled using dry cooling towers. In addition to being highly energy and water efficient, OVHcloud's water cooling technology also has relatively low maintenance costs.

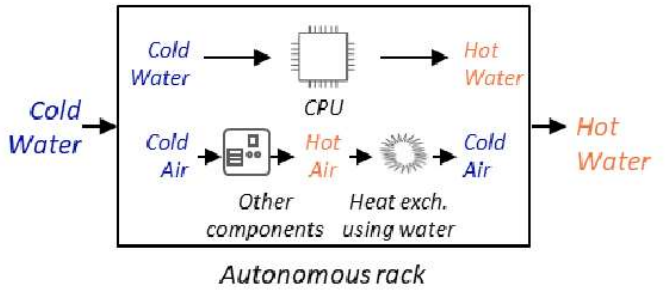


Figure 2: OVHcloud proprietary water-cooling technology principles

In addition, OVHcloud developed its own concept where air-conditioning units were replaced by a natural ventilation system that, thanks to hot and cold airflow, ensured that temperatures were regulated. This concept complemented water-cooling to participate in energy saving.

1.2. OVHcloud Universe of Cloud Offerings

Cloud computing means providing users with storage, computing and network resources, over the internet, on demand. Cloud resources are in data centers that house servers and equipment used to process, store and transmit data. User entities of cloud computing services can access stored data and instruct processing units to perform computing functions automatically, without the need for human interaction, minimizing the computing and storage capacities needed on their devices (such as personal computers, tablets and mobile phones). Wherever they are located, so long as they have an internet connection, user entities can access IT services through the cloud.

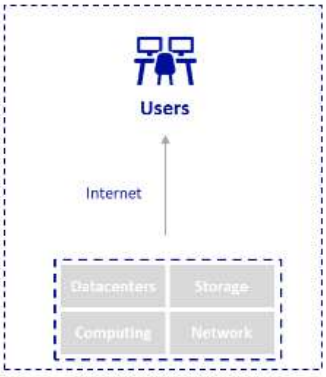


Figure 3: Basic structure of a cloud computing system

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Servers maintained in data centers can be used for multiple functions, each of which is accessed through a "virtual machine" created on the server. The virtual machines are operated and separated from one another through a software platform known as a "virtualization stack." Each virtual machine can have its own operating system that permits user entities to develop and run applications. Through a function known as a "hypervisor," the server's capacity is allocated to the virtual machines in accordance with the demands of user entities. More recently, software applications have been written to be bundled in "containers" that run directly on the operating system of the server itself, coordinated through platforms known as "orchestration" systems, which generally take less space and can provide better performance than hypervisor-based virtualization stacks.

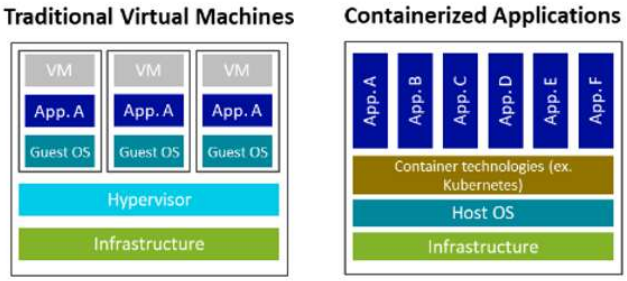


Figure 4: Traditional virtual machine structure and containerized application structure

The ability to create multiple virtual machines on each server or to deploy container-based systems allows a cloud service organization to allocate its capacity among multiple user groups or user entities in a secure manner. Service organizations can dedicate a server to a single user entity (a "private cloud" system), allocating the server's capacity among user groups authorized by the user entity. Alternatively, a server can be shared among multiple user entities (a "public cloud" system). Private cloud user entities generally pay monthly charges for dedicated capacity, whether or not they use that capacity. Public cloud user entities generally pay for the capacity they use.

To optimize the cost of cloud services, many businesses are deploying "hybrid cloud" strategies, in which they combine on-premises or outsourced private cloud capacity for their most sensitive functions and data, with public cloud capacity for their less sensitive needs. User entities are also deploying "multi-cloud" strategies, purchasing cloud services from several user organizations.

The following table summarizes the key features of OVHcloud's main private cloud and public cloud offerings:

	Private Cloud		**Public Cloud**	
	Bare Metal Cloud	**Hosted Private Cloud**	**Virtual Private Servers**	**Shared Public Cloud**
Hardware	Dedicated to user entity		Shared	
Operating system	Selected and managed by user entity	Selected and managed by OVHcloud		
Virtualization Stack	Selected and managed by client (if any)	VMware Hosted and managed by OVHcloud		Hosted and managed by OVHcloud via OpenStack

Cloud computing encompasses a range of services that include providing access to infrastructure (Infrastructure as a Service or "IaaS"), selecting and operating platforms such as operating systems,

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

virtualization stacks and security systems (Platform as a Service or "PaaS"), and offering applications that are developed and can function on cloud platforms (Software as a Service or "SaaS").

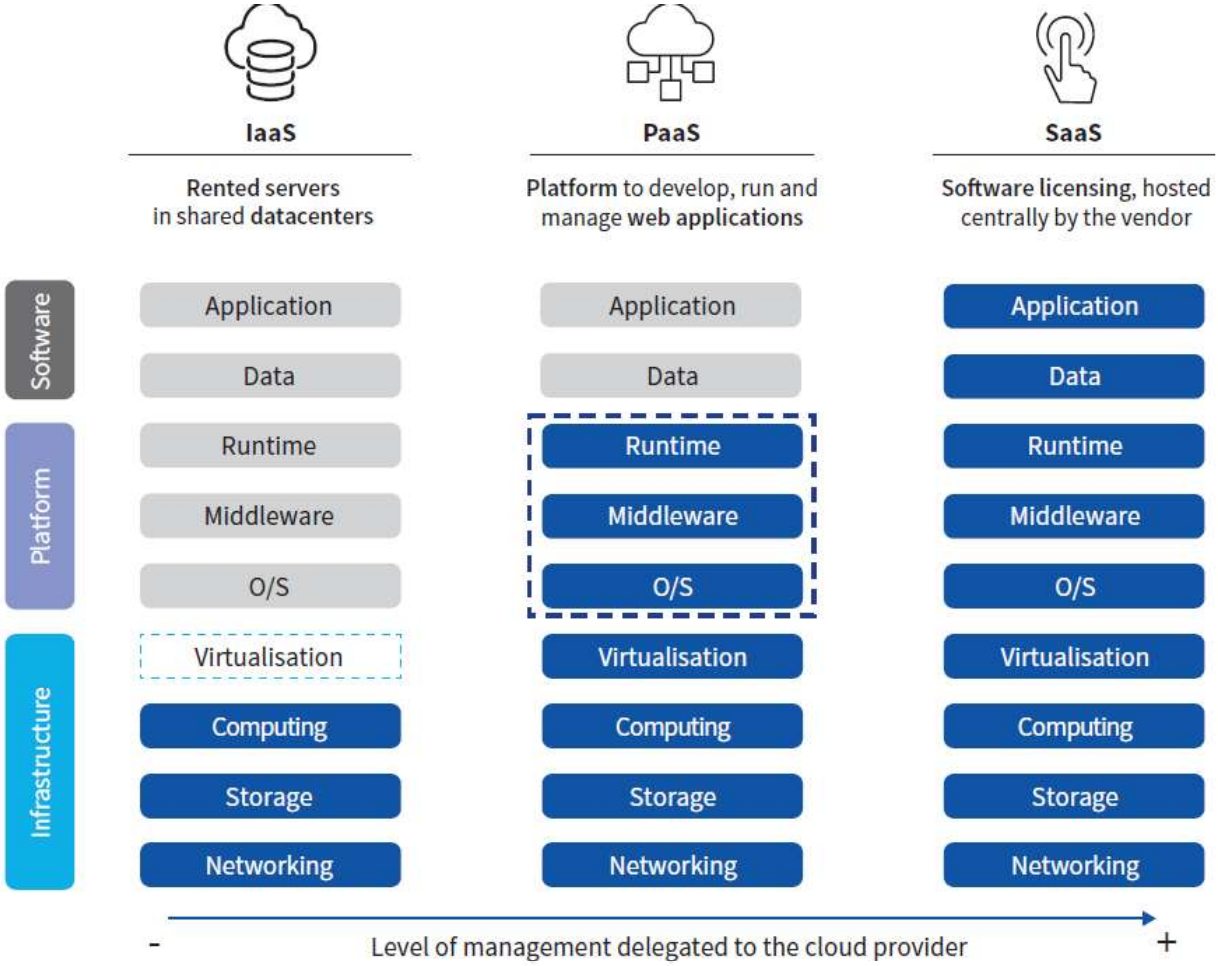


Figure 5: IaaS, PaaS and SaaS features

The cloud solutions market also includes the web cloud market largely consists of web and domain hosting, including renting servers for websites, selling secondary services (such as software packages) and domain name registration, renewal and transfer services.

1.2.1. Bare Metal Cloud

OVHcloud's Bare Metal Cloud service provides dedicated physical servers to user entities, which have full control over the server, including the choice of operating system, which allows them to have an experience similar to what they would have with on-premises solutions managed by their internal IT staff, while taking advantage of the benefits offered by outsourcing.

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

Bare Metal Cloud offers high performance and high scalability with the best price/quality ratio in just a few minutes, for development, production and backup. Highly reliable, customizable and scalable, Bare Metal Cloud provides user entities with instant provisioning and fully automated access to dedicated servers on which the user entity operates and manages all software layers, including the operating system.

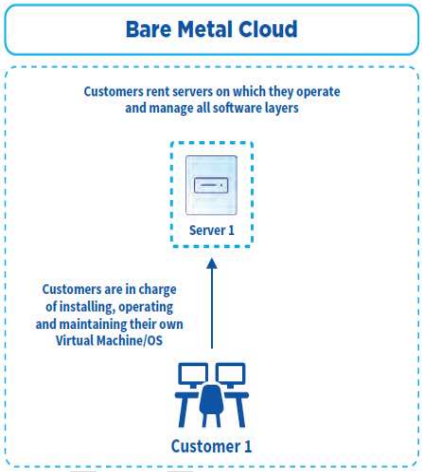


Figure 6: Bare Metal Cloud service

Bare Metal cloud services provide user entities with high-level computing power and strict Service Level Agreements, in a secure environment appropriate for data-sensitive applications. The server can be customized to meet user entity requirements and can be operated without a need to allocate the server's capacity to virtual machines through a hypervisor, which allows the customer to use the server's full capacity. Any unused capacity can be deployed within minutes, although the total capacity is limited by that of the dedicated server. Bare Metal user entities are typically responsible for making their own data backup arrangements, although they can also choose from several backup options offered by OVHcloud (with backed-up data stored within the same data center or at a different location). Bare Metal cloud user entities may choose various additional service options such as specific performance levels, server customization or data backup.

Bare Metal Cloud services provide security, performance, customization and cost effectiveness, and are typically used for data intensive operations such as media encoding (like 3D animation), media streaming, complex data-computing (such as analyzing oil and gas field seismic data), low latency operations such as high frequency trading, media streaming, online gaming and online advertising, critical corporate applications requiring high-security operations such as ERP and CRM system operations, specialized applications such as customized Internet-of-Things, and applications designed to meet strict regulatory compliance requirements in highly regulated sectors.

1.2.2. Hosted Private Cloud

OVHcloud offers hosted private cloud services in a fully dedicated environment providing dedicated servers and platforms fully managed by OVHcloud, including the operating system and the virtualization stack (using VMware technology).

OVHcloud's hosted private cloud services provide user entities with private access to servers that can be customized to meet the user entities' specific requirements. The server provides high performance, although slightly below that of high-end Bare Metal cloud service, because the hypervisor uses some of the server's capacity. It meets the needs of user entities seeking isolation and security, scalable resources (within the limits of the server's capacity) and resilience.

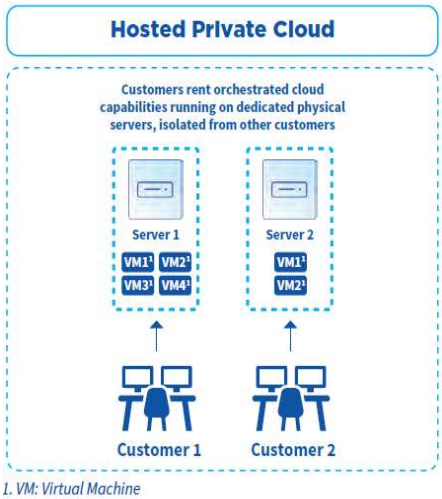


Figure 7: Hosted Private Cloud service

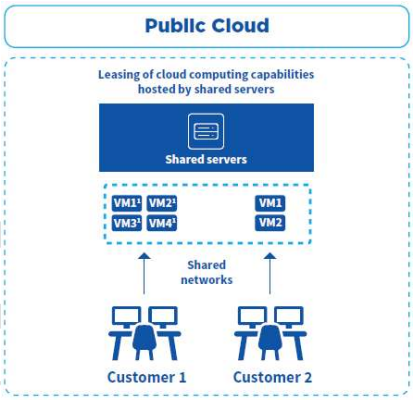
The main usages for hosted private cloud services include deployment in hybrid cloud strategies, media encoding, big data analytics and disaster recovery, as well as the storage and processing of sensitive data in key sectors such as healthcare, finance and the public sector.

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

1.2.3. Public Cloud

OVHcloud offers public cloud solutions based on open-source technologies such as OpenStack (a platform that controls diverse, multi-vendor pools of processing, storage, and networking resources) and Kubernetes (an industry standard container orchestration platform). The use of these standard platforms provides user entities with easy data transfer capability and access to source code, facilitating reversibility and eliminating "vendor lock-in". It is particularly adapted for user entities seeking to deploy hybrid cloud strategies.

Public cloud solutions provide users with virtually unlimited computing capacity, with the only constraint being the demands of other users and the total installed capacity of the cloud provider.



1. VM: Virtual Machine

Figure 8: Public Cloud service

Capacity can generally be accessed automatically in seconds. Because public cloud service is based on shared servers offering user entities the highest degree of scalability and continuity, customization options are limited. OVHcloud provides high SLAs given the flexibility of the hardware architecture.

Public cloud offering provides three core cloud computing services: computer performance, storage and network capabilities. It also provides five additional, high-level services: orchestration and containerization, including tools to manage processes and software stacks; data analytics, including data collection and processing services; artificial intelligence, including automated deployment, launch, training and evaluation of machine learning models; management interfaces; and project management solutions. User entities of OVHcloud public cloud solutions can choose a virtual private server option, providing computing capabilities located on shared servers, but with "virtual machines" isolated using virtual private networks.

The virtual private server option is particularly adapted for user entities seeking tailored resources, particularly for short-duration operations with volatile workloads and server demand across multiple access locations, and a high degree of resilience. Virtual private server solutions are used primarily for applications testing and other one-time projects, the management of short-duration peak loads and backup functions. OVHcloud also offers fully scalable public cloud services on virtual machines that are housed on share servers but are not isolated through virtual private networks. This service is used for applications with high demand bursts (such as e-commerce websites) and services that use large volumes of data, such as video and music streaming. Public cloud services can also be used by user entities for workloads that are not sufficiently mission-critical to warrant the use of private cloud resources.

1.2.4. Platform-as-a-Service Solutions

OVHcloud provides PaaS offers on its private cloud and public cloud IaaS products, primarily in the following areas:

- **Artificial Intelligence and Analytics**: Artificial intelligence and analytics solutions include tools and services supporting data analysis and data presentation, such as the management of end user queries, data labelling, and image and text presentation. OVHcloud is active in providing high performance computing solutions for artificial intelligence and machine learning and intends to pursue its development in this area.

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

- **Data Management Software**: Data management software allows users such as database managers and developers to manage databases to allow for queries and random updates, and it represents the largest single segment of the PaaS market. It includes programs that execute queries on data and provide visual representation of the data in formats such as spreadsheets, enabling users to build applications faster and automate database management.
- **Application Platforms**: Application platforms are back-end server software solutions providing developers with a cohesive application execution environment (e.g. application execution, access to data, authentication coordination, session management). OVHcloud integrates key application platforms from VMWare.
- **Web cloud Platforms**: beyond its web cloud offer, OVHcloud provides an end-to-end web platform
allowing developers to build, run and scale applications.
- **High Performance Storage**: including Block Storage, Object Storage and Cold Archive.
- **Security and Encryption**: including identity access management and encryption solutions, including end-to-end encryption.

1.2.5. Web Cloud

OVHcloud has offered web cloud services since its founding in 1999. OVHcloud provides user entities with web cloud services, including website hosting and domain registration, telecommunications and internet access, as well as a "marketplace" for third-party software solutions to help user entities empowering their digital journey.

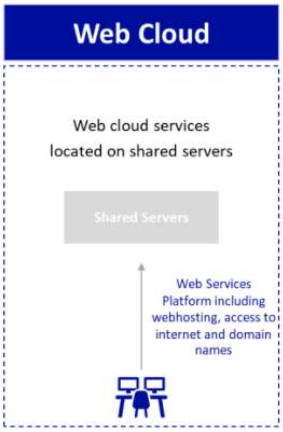


Figure 9: Web Cloud service

OVHcloud offers three principal solutions to web cloud user entities:

- **Web hosting and domain registration**: This includes the rental of capacity on web servers, allowing user entities to connect their websites to the internet, as well as domain name registration, renewal and transfers together with email addresses and storage options. OVHcloud offers web hosting customers additional services, such as Secure Socket Layer (SSL) certificates, which allow secure connections from a web server to a browser.
- **Telephony and Network**: User entities may purchase Voice over IP systems providing phone numbers and unlimited calls to fixed lines (and, in the high-end package, mobile lines), and enabling usages such as telephone switchboards and interactive voice response systems. OVHcloud also provides large-volume telephony options that are capable of handling video and other media. OVHcloud also offers customers internet access through ADSL and fiber networks, with basic and professional packages.
- **Software Marketplace**: Web cloud user entities have access to OVHcloud's software marketplace, providing more than 250 fully digital SaaS and PaaS solutions with 6 categories from third-party vendors that can run on OVH's infrastructure, in areas such as collaboration, emailing and social networking, managed services (such as outsourcing), corporate tools (business intelligence, CRM and ERP), coding and applications development, and solutions for specific industries such as e-learning, healthcare, legal and real estate.

1.3. Scope Covered in this Report

Our service "Public Cloud Infrastructure" provides a wide variety of cloud services integrated with each other, forming a coherent offer of infrastructure as a service. The core of the service is built with

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

Openstack and consists in compute, block storage and object storage. Specifically, it provides the following services and features:

- Public Cloud **Compute** is a platform that uses pooled virtual resources to build and manage public clouds. The tools that comprise the PCI platform, called "projects," handle the core cloud-computing services of computer, networking, storage, identity, and image services. PCI Compute service provides three kind of instances that aim at different goals:
  - balanced instances: Catalogue of top-range instances, with fully guaranteed resources. General Purpose instances have a balanced distribution of resources and suit most uses. CPU instances are particularly powerful in terms of computing capacity. As for RAM instances, they offer a very high volume of memory.
  - IOPS instances: IOPS instances deliver the fastest disk transactions in the Public Cloud range. They offer direct access to NVMe drives, each of which deliver at least 400,000 read/write operations per second. These cloud solutions are designed to host database (DB) servers and big data applications.
  - GPU instances: GPU instances integrate NVIDIA Tesla V100S graphic processors to meet the requirements of massively parallel processing. These cloud servers are adapted to the needs of machine learning and deep learning.
- **Object Storage** (Swift / OpenIO) offers a high-performance, scalable and secure storage space. It allows the user to upload static files (videos, images, web files) to an unlimited space and use them from an application or make them accessible on the web via a S3 API. This storage space can be scaled up as the project grows, with no need to plan for it in advance. It can meet the requirements of big data, artificial intelligence (AI) and document catalogues, or simply help to get the most out of csutomers' data. Object Storage also includes **Cold Archive** service, which provides long-term, cost-efficient storage. Data is stored on an S3 buffer before being sent to magnetic tapes in smaller scale datacenters, dedicated to this service.
- **Block storage** Ceph-as-a-Service (CaaS) is a framework that can deploy and maintain Ceph based clusters. Ceph is a unified, distributed storage system designed for excellent performance, reliability and scalability and Ceph-as-a-Service is a system for complete life-cycle management of Ceph clusters. When persistent storage requirements increase, the user instantly meets growing demands by hot-adding extra disks to increase the instance's capacity. These volumes are securely hosted in OVH's clusters and can be used to meet the requirements of applications that handle large volumes of data.

The billing is based on the volume and typology of services consumed; a key component is pay-as-you-go, meaning that only resources consumed are billed, and hourly billing is available. See https://www.ovhcloud.com/fr/public-cloud/prices/ for details. Entry-level offers are affordable; therefore Public Cloud clients range from small entreprise to large accounts.

We also provide Platform-as-a-Service (PaaS) products that are built on top of Public Cloud Infrastructure products. These products are hosted on Public cloud instances and are preconfigured to provide specific services.

- Kubernetes:
  - **Managed Kubernetes** (K8s) which is the industry-standard container orchestrator, used by companies of all sizes. It facilitates the deployment, resiliency and scalability of the customer's applications, even in hybrid or multi-cloud infrastructures. The "Managed Kubernetes" solution is powered by OVH's Public Cloud instances. OVH deploys, hosts and maintains all the components needed for Kubernetes to work, including updates linked to bugs and security patches. OVH also maintains the necessary components on the customer's nodes. Kubernetes launches containers and configures the Load Balancer for the customers, and they can instantly add new computing nodes. The customers can also define the health conditions for each service, after which Kubernetes will relaunch any pods and containers that do not meet these criteria. The customers' nodes can be monitored, and their services benefit from the high availability of OVH Infrastructure-as-a-Service (IaaS) solutions.
  - **Private registry**, which enables customers to host helm charts and docker images
  - **Rancher** simplifies the management of multiple Kubernetes clusters, particularly in a multi-cloud or hybrid cloud approach.

First version

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

- Databases & Analytics:
  - **Cloud Databases**: offers a fully managed database service. The customer is billed hourly according to the resources he ordered.
  - **Dataplatform:** a unified platform for integrating, storing, preparing, and leveraging customers' data to speed up data and analytics projects.

- AI Products provide a fast and easy way to get through a Artificial Intelligence pipeline. This offer is split into four products **AI Notebook**, **AI Training**, **AI Deploy and AI Endpoints**. The computer engine is based on Kubernetes. The customer is billed by the minute and only for what resources he consumes. AI Products enables clients to leverage GPU hardware simply and without compatibility headaches.

- Logs Data Platform is a platform that allows to manage logs. It ingests the logs generated by infrastructure and applications, stores them, displays them in real-time dashboards and allows users to perform complex queries.
  Logs Data Platform can also be used as a powerful indexing platform for any kind of document.
  To operate Logs Data Platform, OVHcloud leverages various Open-source Software such as OpenSearch, Logstash, Flowgger, etc to bring many features to the customers and guarantee interoperability with most of the softwares on the market.

Several services and features are included in the Openstack framework and thus available in all Public Cloud projects by default.

- Identity service (Keystone)
- Managed private registry and public catalog
- WebUI service
- Network connectivity (Neutron)
- Metering service (Ceilometer)
- Roles and Rights Management
- Workflow management (Mistral)

Public Cloud scope	Product name	ovhcloud.com page	Commercial offers
Public cloud Compute	Public Cloud Instance	https://www.ovhcloud.com/fr/public-cloud/compute/ https://www.ovhcloud.com/fr/vps/ https://www.ovhcloud.com/fr/public-cloud/metal-instances/	Cloud GPU Instances Metal Instances VPS
Object Storage	Object Storage	https://www.ovhcloud.com/fr/public-cloud/object-storage/	Cloud Archive Object Storage Object Storage Swift
	Cold Storage	https://www.ovhcloud.com/fr/public-cloud/cold-archive/	Cold Archive

Final version
hf195743ovh

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Block Storage	Block Storage	Dedicated : https://www.ovh.com/fr/cloud-disk-array/ Public: https://www.ovhcloud.com/fr/public-cloud/block-storage/	Cloud disk Array, Block Storage
Kubernetes	Managed Orchestration	https://www.ovhcloud.com/fr/public-cloud/kubernetes/ https://www.ovhcloud.com/en/public-cloud/managed-rancher-service/	Managed Kubernetes Service, Managed Rancher Service
	Managed OCI artifact Registry	https://www.ovhcloud.com/fr/public-cloud/managed-private-registry/	Managed Private Registry
Data / Cloud Databases	Managed Search Engine Software Platform	https://www.ovhcloud.com/fr/public-cloud/opensearch/	Opensearch
	Managed In-Memory Database	https://www.ovhcloud.com/fr/public-cloud/redis/	Valkey
	Managed Document Database	https://www.ovhcloud.com/fr/public-cloud/mongodb/	MongoDB
	Managed Relational Database	https://www.ovhcloud.com/fr/public-cloud/mysql/ https://www.ovhcloud.com/fr/public-cloud/postgresql/	MySQL PostGreSQL
	Managed Column-Oriented Database	https://www.ovhcloud.com/fr/public-cloud/apache-cassandra/	Cassandra
	Managed Message Broker	https://www.ovhcloud.com/fr/public-cloud/apache-kafka/	Managed Kafka
	Managed Data Visualisation	https://www.ovhcloud.com/fr/public-cloud/grafana/	Managed Dasboards
Data / Dataplatform	Unified Data Platform	https://www.ovhcloud.com/en/public-cloud/data-platform/	

hf195743ovh Final version

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

AI Products	Managed Containers	https://www.ovhcloud.com/fr/public-cloud/ai-deploy/ https://www.ovhcloud.com/fr/public-cloud/ai-training/ https://www.ovhcloud.com/fr/public-cloud/ai-endpoints/	AI Deploy, AI Training AI Endpoints
	Notebook Interface	https://www.ovhcloud.com/fr/public-cloud/ai-notebooks/	AI Notebooks, Quantum Notebooks
Logs Data Platform	Managed Log Manager	https://www.ovhcloud.com/fr/logs-data-platform/	Logs Data Platform

The following business processes are considered to be part of the scope:

- The provision, connectivity, maintenance in operational conditions and decommissioning of the infrastructure allocated to the customer.
  - Provision of the infrastructure allocated to the customer
  - Connectivity of the infrastructure allocated to the customer
  - Maintaining the infrastructure allocated to the customer in operational and security conditions
  - Decommissioning of the infrastructure allocated to the customer at the end of the service
- The means provided to the client for the configuration, use and monitoring of the allocated platform.
  - Configuration of the infrastructure and options by the customer
  - Use and administration of the infrastructure by the customer
  - Monitoring of the infrastructure by the customer

2. Components of the System Used to Provide the Services

Public Cloud Services System is comprised of the following components:

- **Infrastructure:** computer equipment (e.g., servers, network and storage devices) and physical technology upon which the system is hosted.
- **Software:** application programs and system software used to deliver the services.
- **People:** personnel involved in the governance, operation, and use of the system and delivery of services.
- **Procedures:** automated and manual procedures to operate, maintain, and secure the services.
- **Data:** transaction streams, files, databases, tables, and output used or processed by the system.

These components are described in further detail below.

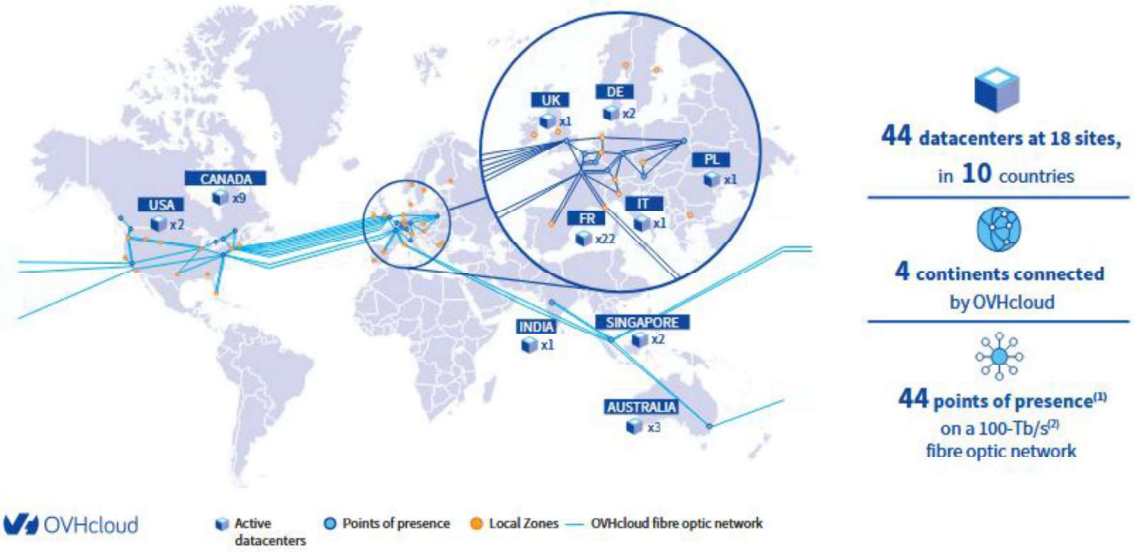
2.1. Infrastructure

OVHcloud has multiple clouds around the world, each operating from a Point of Delivery (POD). A POD is a standardized design of equipment and software that provides the in-scope cloud services. A POD

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

consists of servers, storage and network devices and may vary in size, but the design architecture is similar from site to site.

OVHcloud operates 44 datacenters in 18 locations in Europe, North America, and Asia-Pacific. OVHcloud manufactures its servers in-house and is not dependent on a third-party manufacturer, except for DC tape datacenters and Cold Archive service.



Source: OVHcloud
Notes:
(1) A point of presence is a point at which the network establishes a connection with the Internet.
(2) Tera bits per second.

Figure 10: OVHcloud geographical representation

For Public Cloud products, the following datacenters are used to deliver the service:

Final Version

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

Geographical Area	City	Code	Address	Type
France	Roubaix	RBX	2 rue Kellermann 59100 ROUBAIX	OVH DC
	Gravelines	GRA	ZI des Huttes - Route de la ferme Masson 59820 GRAVELINES	OVH DC
	Strasbourg	SBG	9 rue du Bassin de l'Industrie 67000 STRASBOURG	OVH DC
	DC tape Croix	CRX03	155 avenue Georges Hannart 59170 CROIX	OVH DC
	DC tape Bordeaux	VDO01	Bordeaux	Shell & Core
	DC tape Grenoble	EYN01	Grenoble	Shell & Core
	DC tape Saint-Pierre-des-Corps	SDP01	Saint-Pierre-des-Corps	OVH DC
	3-AZ Paris / Marcoussis	MR901	15 rue Marin Angiboust, 91460 Marcoussis	Colocation SOC report managed by suppliers
	3-AZ Paris / Ferrières-en-Brie	IEB01	16 Av. Joseph Froelicher, 77600 Ferrières-en-Brie	Colocation SOC report managed by suppliers
	3-AZ Paris / Clichy	CCH01	7-9 Rue Petit 92582, Clichy	Colocation
Canada	Beauharnois	BHS	50, rue de l'Aluminerie, Beauharnois QC J6N OC2	OVH DC
	Toronto	YYZ01	7 Vondrau Drive Cambridge, Ontario	Colocation SOC report managed by suppliers
United Kingdom	Erith	ERI	Viking Way 14, Belvedere Link Industrial Estate - ERITH DA8 1EW	OVH DC

final version hf195743ovh

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

Germany	Limburg	LIM	LIMBURG: Limburger Straße 45, 65555 Limburg-Offheim Germany	OVH DC
Poland	Ozarow	WAW	UL. KAZIMIERZA KAMINSKIEGO 6 – 05-850 OZAROW MAZOWIECKI - POLSKA	OVH DC
Australia	Sydney	SYD1	Data Centre SYDNEY - 639 Gardeners Road, MASCOT NSW 2020	Colocation SOC report managed by suppliers
		SYD2	Next DC 6-8 Giffnock Avenue, Macquarie Park NSW 2113	Colocation SOC report managed by suppliers
		SYD3	2 Broadcast Way, Artarmon NSW 2064	Colocation SOC report managed by suppliers
India	Mumbai	MUM	Yotta Datacenter Park - Panvel Hiranandani Fortune City. Survey No. 30, MH SH 76, Panvel, Navi Mumbai, Maharashtra 410206, India	Colocation SOC report managed by suppliers
Singapore	Singapore	SGP1	ALTIMAT Data Center Singapore Pte Ltd - 110 Paya Lebar Road - SINGAPORE 409009	Colocation
		SGP2	23 Tai Seng Drive #06-00, Singapore 535224	Colocation

hf195743ovh
final version

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

2.2. Software

	System				Application	Monitoring and Auditing
	Management tools	*Virtualization and management tools*	*Server operating systems*	*Backup systems*		
Public Cloud-Compute	Puppet Terraform Deployment-as-a-Service (DaaS) MariaDB RabbitMQ	Openstack Nova Qemu (KVM) Kubernetes Docker	Ubuntu	Swift S3	Octavia (HAProxy)	OVH Logs Data Platform Prometheus / Thanos
Public Cloud-Block Storage	Admin servers Puppet	VMs on OVH Private Cloud (PCC - vSphere)	Multiple admins deployed in geographically independent locations with the same accesses so no failover needed Multiple puppet hosts in geographically independent locations. VM disk on PCC datastores which are redundant by design	Code is hosted on stash.ovh.net, database backups hosted on PCS (Swift)	N/A	Icinga2 Opsgenie OVH Logs Data Platform
Public Cloud-Object Storage	Internally developed orchestrators (Mozg) to manage overall infrastructure puppet prefect admin servers	VMs on OVH Private Cloud (PCC - vSphere)	Ubuntu Debian	MySQL dump stored in Swift in another DC VM Managed Backup service provided by PCC	N/A	Icinga2, Opsgenie, OVH Logs Data Platform Prometheus, Grafana, Mimir Tenable, Sonarqube, REVmon

hf195743ovh Final version

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Kubernetes	Ansible Terraform	Openstack Docker Kubernetes	Debian	Etcdctl-backup Internal CriticalDB backup management	N/A	Warp10 Mimir OpsGenie LDP Sentry
Data	Ansible MongoDB OpsManager Terraform Aiven (Aiven is a supplier that provides managed services for databases. SOC controls for this provider are covered by its own SOC2 report)	N/A	Ubuntu running Kubernetes clusters and debian	MongoDump for MongoDB sercices block storage disk snapshot etcd is backuped upon each deployment on a given region, backup is sent to Object Storage S3	Postgresql, MySQL, MongoDB, Valkey, OpenSearch, Apache Kafka, apache MirrorMaker 2, Kafka Connect, Grafana, Cassandra, M3DB, M3 Aggregator AI products (models training jobs, VSCode/Jupyter notebooks, Inference APIs deployments) Apache Spark / Jupiyter	Prometheus and Mimir internal offer for metrics LDP for logs Revmon, Jfrog Xray, CVEmon, Tenable for CVE, sentry
AI products	Ansible MongoDB OpsManager Terraform	N/A	Ubuntu running Kubernetes clusters and debian	MongoDump for MongoDB sercices block storage disk snapshot etcd is backuped upon each deployment on a given region, backup is sent to Object Storage S3	Postgresql, MySQL, MongoDB, , VSCode/Jupyter notebooks, Inference APIs deployments Apache Spark / Jupiyter	Prometheus and Mimir internal offer for metrics LDP for logs Revmon, Jfrog Xray, CVEmon, Tenable for CVE, sentry

Final Version hf195743ovh

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Logs Data Platfom	Puppet OpenSearch Graylog Flowgger Logstash	Kubernetes Docker	Debian	S3 MongoDump for MongoDB Rsync	MongoDB PostgreSQL LDAP Kafka HAProxy	Shinken Opsgenie Quality Pingdom Prometheus Revmon Jfrog Xray CVEmon Tenable scans Syslog Splunk

2.3. People

OVHcloud's mission and core values are carried out by OVHcloud people with respect to integrity, ethical values, management's operating style, delegation of authorities, as well as overall the organization processes set by the Governance.

All personnel are provided with the legally binding Code of Ethics and IT Charter before following onboarding and awareness training. OVHcloud made available an Ethics and Compliance hotline for personnel to anonymously report on possible violations or misconduct. All contracts include non-disclosure requirements and personnel are made aware that any confidentiality breach, violation or misconduct may lead to a disciplinary action which might cause an immediate dismissal. Throughout the hiring process, a staff screening is performed ensuring new hires would fit their role based on knowledge and experience proportionally to the position they would take at OVH-cloud. Staff screening also includes background checks in line with local laws and regulations.

Management distributes roles and responsibilities based on the skillset appropriateness to best combine the skills and experiences of key staff between management, system and software development and maintenance skills. As part of their onboarding, new personnel are trained on OVH-cloud security and control measures that have been defined by management. Regular management and one-to-one meetings are held ensuring continuous feedback and team development in order to support OVHcloud objectives and security measures.

2.3.1. Organizational Structure

The following organization chart illustrates OVHcloud's organizational structure:

- The BU Commerce is responsible for selling OVHcloud solutions to customers, providing them support, animating an ecosystem of offers and partners.
- The BU Product is responsible for developing, automating and operating the cloud infrastructures and platform, relying on industrial standards and based on customer and market feedback.

Final version

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

- The BU Industry is the infrastructure architect and operator of OVHcloud from engineering to server manufacturing, from infrastructure design to data centre management ensuring the level of quality and availability of the infrastructures adapted to the services expected by OVHcloud customers.
- The BU Ops is responsible for coordinating and ensuring that the company's resources are aligned with its objectives by streamlining the organization, providing information systems, automating processes via lean management, and facilitating cooperation between the BUs.
- The BU Corporate consists of the Finance, HR and Legal management functions.

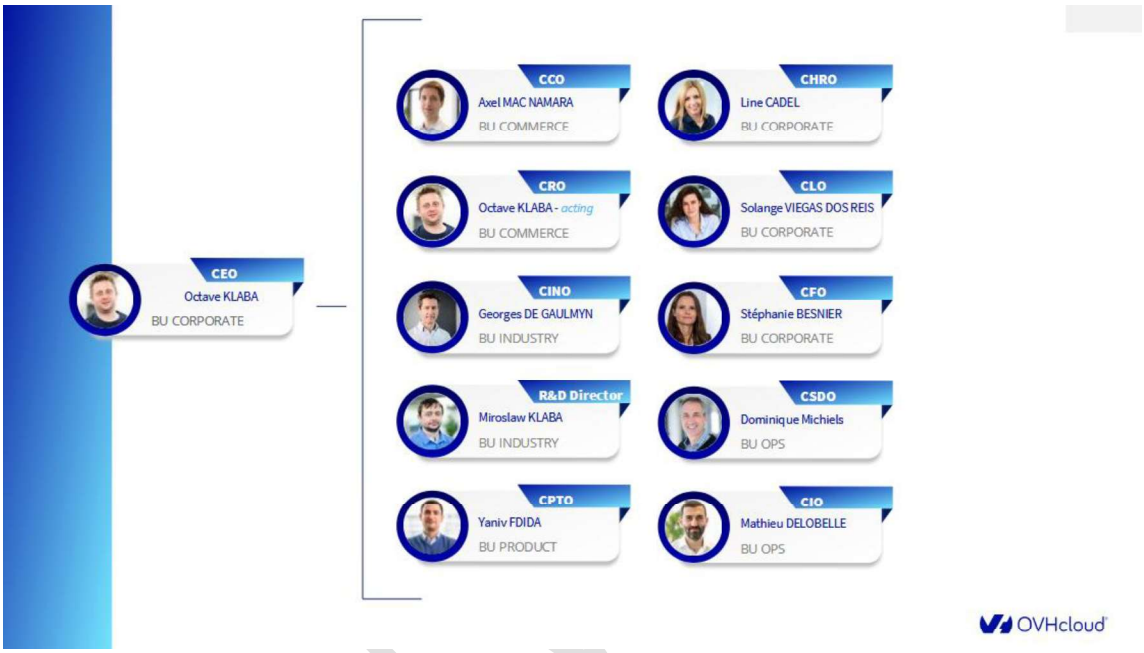


Figure 11: OVHcloud organizational structure

2.3.2. Governance

Governance sets the tone at the top as a foundation of OVHcloud's mission and core values. OVHcloud operates under the management of an Executive Committee committed to the Group's mission to provide customers around the world with secure, trusted, open, sustainable cloud solutions. In addition, the Group is overseen by a Board of Directors composed of independent *administrateurs*. An overview of the members can be found here: https://corporate.ovhcloud.com/en-ie/company/governance/.

OVHcloud corporate governance has established, maintains and monitors standards for integrity, ethical values, management's operating style, delegation of authorities, as well as overall organizational processes. For that purpose, OVHcloud governance has distributed appropriate roles and responsibilities within the organization:

- The Chief Information Security Officer (CISO) to oversee the information security program and who is supplemented by a security team responsible for centralizing the global coordination of information security within OVHcloud including:
  - Dedicated Security Managers responsible for determining, implementing, maintaining and monitoring appropriate and relevant state-of-the-art security measures;
  - A Risk Manager who coordinates the management of security risks and the associated action plans;

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

- The Data Protection Officer to oversee all topics related to privacy;
- A network of Security and Privacy referents within the different BUs responsible for security and privacy topics within their scope; they ensure the link between the security and privacy teams with the Product and IT teams;
- An Ethics and Compliance team to oversee the ethics and compliance topics.

2.4. Procedures

2.4.1. Policies and Procedures

OVHcloud has developed and maintains its Information Systems Security Policy made publicly available on OVHcloud website: https://docs.ovh.com/gb/en/security/issp/. The ISSP provides the security reference framework to which OVHcloud management is committed towards all OVHcloud stakeholders.

Beyond the main policy setting the security concepts and approach, OVHcloud is organized by security themes adapted to OVHcloud organization and operations with dedicated security procedures and controls:

During the year 2023, the 28 security themes were redesigned:

1	Define and maintain security governance (Security governance)
2	Maintain consistent security principles and documentation (Security model)
3	Provide to customer appropriate security features to manage their risks (Customer Security Features)
4	Implement appropriate data protection for any data managed or hosted (Data Protection)
5	Demonstrate compliance with OVHcloud commitments (Security compliance)
6	Promote risk-based decisions (Security risks management)
7	Build, develop and maintain relationship with security ecosystem (Security ecosystem)
8	Protect customer's cloud usage (Security Protection for Customer)
9	Protect OVHcloud technical reputation (External technical reputation)
10	Assess security and implement continuous improvement (Audits and controls)
11	Assets management
12	Ensure alignment of resources with security objectives and develop a security culture (Human resources, Awareness and Training)
13	Identity, Authentication and Access Management
14	Protect end-user information system (End user information system)
15	Supply Chain and Service Provider Management
16	Support IT and product developments (Project management)
17	Manage security in IS evolution (Change management)
18	Secure continuous delivery
19	Use strong Cryptography (Cryptography)

Final version

hf195743ovh - mediaxGmbH - 2026-10-02 - Confidential - TLP:GREEN

20	Deploy and maintain secure configuration and hardening (Configuration and hardening)
21	Ensure Network security (Network security)
22	Operations and Maintenance in Security Conditions
23	Logging, security monitoring and detection
24	Vulnerability and patch management
25	Security incident management
26	Datacenter security
27	Office security
28	Resilience

In a fast-moving world where change is the only constant, security practices must constantly evolve to remain relevant and adapted to its environment. As a result, OVHcloud security policies, procedures and controls are subject to a constant evolution to maintain state-of-the-art security practices.

2.4.1.1. Automated Procedures

The automated procedures consist of programmatic controls developed and incorporated into the system, as well as network, infrastructure, server and system software support and monitoring tools. The key automated processes and tools include:

- User authentication and access controls
- Scheduled system and infrastructure backup processes
- Automated system monitoring and logging
- Automatic alerting (for security and availability)

2.4.1.2. Manual Procedures

Manual processes (supported by policies, procedures, and guidelines) for operating and maintaining the system, including processes for:

- User administration processes
- Security and vulnerability management processes
- Service desk processes
- Client delivery, onboarding and system configuration processes
- Client decommissioning processes
- Change management processes
- Security Monitoring
- Patch updates and change control processes
- Physical security processes
- Technical configuration baselines

hf195743ovh Final version

hf195743ovh - medhexGmbH - 2026-10-02 - Confidential - TLP:GREEN

- Incident and problem management processes
- HR procedures, including background checks and performance reviews
- Business Continuity and Disaster Recovery procedures

2.5. Data

The key types of data collected, processed, and stored by the Public Cloud Services System include:

- Server and network configurations
- Custom parameters for client configurations
- Client information specific to access control, including usernames
- Client personal data specific to support and billing
- Logs of all infrastructures, including customers infrastructures

This data is collected, processed and stored to guarantee the provision, connectivity and maintenance in operating condition.

Final version
hf195743ovh

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

Attachment 2 - Principal Service Commitments and System Requirements

OVHcloud establishes policies and procedures for the Public Cloud Service System to meet its objectives for providing cloud and data services. Those objectives are based on: (i) principal service commitments and requirements made to user entities; (ii) laws and regulations governing the provision of such services; and (iii) other financial, operational, and compliance requirements that OVHcloud has established for these services.

The principal service commitments and system requirements for the Public Cloud Services System include but are not necessarily limited to:

- Security practices within the design, implementation and operation of the Public Cloud Services System are adopted to secure data from unwanted access through access control, technical infrastructure control, encryption, monitoring, and policies and procedures.
- Availability practices within the design, implementation and operation of the Public Cloud Services System are adopted to reduce the likelihood and impact of system inaccessibility through capacity management, backup strategies, and business continuity planning.
- Confidentiality practices within the design, implementation, and operation of the Public Cloud Services System are adopted to identify confidential information classified according to the TLP protocol and apply protection against unauthorized disclosure, through policies and procedures, data classification, security controls, and data destruction.
- Privacy practices within the design, implementation and operation of the Public Cloud Services System are adopted to put in place protection controls to protect Personally Identifiable Information (PII) as a cloud PII processor considering 3 main sources of requirements:
    - Legal, statutory, regulatory and contractual requirements;
    - Risks;
    - Corporate policies.

OVHcloud establishes operational requirements that support the achievement of its security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the company's policies and procedures, design documentation, and contracts with customers. Information security and availability policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Storage Services System.

hf195743ovh
Final version

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Attachment 3 - OVH Groupe S.A.'s Complementary User Entity Controls

OVHcloud services were designed with the assumption that certain policies, procedures and controls are implemented by its customers in a principle of shared responsibility between OVHcloud and its customers. While OVHcloud achieves the objectives described in Section III, the overall achievement of the control objectives also depends on the policies, procedures and controls implemented by user organizations. As such, user organizations are responsible for the design, implementation and operation of their OVHcloud environment according to the level of service they have chosen. Therefore, user organizations are responsible for evaluating their own internal control to determine whether the identified Complementary User Entity Controls have been appropriately designed and operating effectively, where applicable.

The list of Complementary User Entity Controls presented below does not represent all control considerations required by user organizations as other controls may be required in line with the user organization's characteristics.

	Complementary User Entity Control Considerations	Associated Criteria
	General	
1	User organizations should maintain formal policies that provide guidance for information security within the user organization and the supporting IT environment.	CC1.5, CC5.3
2	User organizations are responsible for identifying and establishing adequate controls in line with responsibilities defined as per the contractual agreement and the Data Protection Agreement signed with OVHcloud.	CC1.1, CC1.3, CC1.5
3	User organizations should assess whether the security control objectives applied by OVHcloud are relevant to the risks associated with the way they use their OVHcloud infrastructure. Therefore, user organizations are responsible for identifying the risk and corresponding controls to be implemented to address those risks when using OVHcloud services, software and implementing OVHcloud operational controls.	CC3.1, CC3.2, CC3.3
	Access	
4	User organizations are responsible for establishing appropriate controls and measures allowing relevant access to the environment provided by OVHcloud.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

5	User organizations are responsible for using strong authentication methods to their OVHcloud environments such as multi-factor authentication or strong passwords.	CC6.6
6	User organizations are responsible for establishing appropriate access controls over the use of their OVHcloud environments such as security groups, Identity Access Management and/or Access Controls Lists and Segregation of Duties.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7
7	User organizations are responsible for reviewing the access rights and logs associated with their OVHcloud accounts.	CC6.1, CC6.3
8	User organizations are responsible for granting and disabling access to their OVHcloud services when necessary.	CC6.3, CC6.5
9	User organizations are responsible for ensuring the supervision, management and control for access to key systems hosted in the OVHcloud environment.	CC6.1, CC6.3, CC7.2
10	User organizations must ensure that their workstations and mobile equipment are secure to enable the administration tasks of their OVHcloud service and related systems in line with the criticality of their environment.	CC6.1, CC6.6, CC6.8
	Security events, backup and patching	
11	User organizations are responsible for monitoring security related events and logging appropriate diagnostic information of their systems in their OVHcloud environment.	CC7.1, CC7.2, CC7.3
12	User organizations are responsible for identifying and patching vulnerabilities as well as ensuring periodic maintenance on their OVHcloud environment in line with responsibilities defined as per the contractual agreement.	CC7.1, CC7.2
13	User organizations are responsible for establishing their own backup and restoration processes in the event of loss or damage to their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	A1.2, A1.3
14	User organizations are responsible for implementing their own Disaster Recovery and Business Continuity Plans that address the inability to access or utilize their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	CC9.1, A1.2, A1.3

Final version

hf195743ovh - mediexGmbH - 2026-10-02 - Confidential - TLP:GREEN

15	User organizations are responsible for ensuring that their OVHcloud resources have the appropriate levels of redundancy and isolation; redundancy can be achieved using multiple locations.		CC9.1, A1.1, A1.2
16	User organizations are responsible for implementing appropriate incident response processes.		CC7.4, CC7.5
	Change management		
17	User organizations are responsible for following appropriate security practices during development and deployment of their systems in the OVHcloud environment.		CC8.1
18	User organizations are responsible for appropriately testing and approving changes on their systems before being deployed in their OVHcloud environments.		CC8.1
	Data and Privacy		
19	User organizations are responsible for managing compliance with applicable laws and regulations (including the General Data Protection Regulation).		P1.1, P2.1, P4.2, P6.6
20	User organizations are responsible for the integrity and the content of the data stored in their OVHcloud environment and the data transfers from their OVHcloud environment to an external environment. User organization should establish adequate controls for ensuring data integrity and compliance with applicable regulatory requirements.		CC6.7
21	User organizations are recommended to use encrypted (TLS/SSL) connections for all their interactions with OVHcloud. User organizations are responsible for determining, implementing and managing encryption requirements in their OVHcloud environment when it is not enabled by default and / or can be controlled by user organizations.		CC6.7, CC6.8
22	User organizations are responsible for managing IP resources in an appropriate and sufficient manner to ensure the proper functioning of the OVHcloud services they subscribed to.		CC6.7, CC6.8
	Public Cloud specifics		
23	Compute	User organizations are responsible for installing and managing operating systems and applications on their instances.	CC6.1, CC5.1
24		User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3

Final version

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

25		User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
26	Block Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
27	Object Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
28	Managed Kubernetes	User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3
29		User organizations are responsible for not altering the pre-configured systems that operate the Kubernetes cluster.	CC5.1, CC5.2, CC6.1
30	Private Registry	User organizations are responsible for the lifecycle of the images stored in their private registry; user organizations are responsible for ensuring their images are devoid of security vulnerabilities or malware.	CC5.1, CC6.6, CC7.2
31	Data	User organizations are responsible for their use of the Service, managing data lifecycle and encryption.	CC6.7
32	Logs Data Platform	User organizations are responsible for their use of the Service, managing data lifecycle and encryption.	CC6.7, CC6.8

Public Cloud Specifics

Compute

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-instances-raci?id=kb_article_view&sysparm_article=KB0054604.

Block Storage

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-block-storage-raci?id=kb_article_view&sysparm_article=KB0054797.

Object Storage

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-storage-shared-responsibility?id=kb_article_view&sysparm_article=KB0057223.

Managed Kubernetes

Final version
hf195743ovh

hf195743ovh - mediteXGmbH - 2026-10-02 - Confidential - TLP:GREEN

Further details on user organizations responsibilities are detailed on : https://help.ovhcloud.com/csm/en-gb-public-cloud-kubernetes-responsibility-model?id=kb_article_view&sysparm_article=KB0058751.

Private Registry

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-private-registry-responsibility-model?id=kb_article_view&sysparm_article=KB0058675.https://support.us.ovhcloud.com/hc/en-us/articles/19654193732627-Responsibility-Model-Managed-Private-Registry-Harbor

Data

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-databases-responsibility-model?id=kb_article_view&sysparm_article=KB0036388.

Logs Data Platform

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/fr-logs-data-platform-responsibility-model?id=kb_article_view&sysparm_article=KB0037685

Final version
hf195743ovh

hf195743ovh - medflexGmbH - 2026-10-02 - Confidential - TLP:GREEN

Final Version

OVHcloud

© 2026 OVHcloud, OVHcloud.com. All rights reserved. The OVH name and logo are registered trademarks or trademarks of OVH Group S.A.