

Comparison of European Cloud Providers

Data Sovereignty in Practice

Executive Summary

The US CLOUD Act means that data on infrastructure of American cloud providers can fall under foreign jurisdiction, even when it is located in Europe. For organisations working with sensitive personal data, this is a tangible risk. Commissioned by the Municipality of Nijmegen, T&T Data Consultancy investigated in October 2025 which European cloud provider is the best fit for a sovereign data platform.

Five European providers – OVHcloud, Scaleway, STACKIT, T Cloud Public and UpCloud – were assessed against 24 criteria across sovereignty, security, services, cost and support. The two highest-scoring candidates (T Cloud Public and Scaleway) were additionally validated by building a proof-of-concept environment.

T Cloud Public (TCP) by Deutsche Telekom scores best: fully owned data centres with three availability zones in the Netherlands, no sub-processors, the most mature IAM model, Entra ID integration and a well-documented Terraform provider. Scaleway was eliminated in practice due to insufficient Terraform support. The remaining providers scored insufficiently on access management, Infrastructure-as-Code or connectivity.

The differentiator between European cloud providers is not in basic services, but in access management, integration with identity systems, maturity of managed services and Infrastructure-as-Code.

Based on the assessment and practical validation, the Municipality of Nijmegen was advised to build the data platform on **T Cloud Public**. The European cloud market is evolving rapidly; periodic reassessment of this choice is recommended.

The cloud market is dominated by a limited number of American hyperscalers: AWS, Microsoft Azure and Google Cloud. Although these providers are technologically mature, their dominant position brings legal, strategic and geopolitical dependencies.

At the same time, European cloud providers are developing at a rapid pace. Where they were previously primarily IaaS providers, they now offer an increasingly broad portfolio of managed and supporting services. Therefore, more and more organisations are asking themselves:

How do we build a future-proof data platform within European jurisdiction, without compromising on maturity, security and scalability?

This whitepaper is intended as a practical reference framework for organisations that want to make a well-considered choice for a European cloud. In doing so, we share our experiences from a concrete selection and implementation process at the Municipality of Nijmegen.

This research was conducted in **October 2025**. Developments are following each other in rapid succession. It is therefore always advisable to verify whether certain exclusion criteria still apply.

1. Why Data Sovereignty Matters Now	3
2. The Compared Cloud Providers	3
3. Cloud Provider Maturity	4
4. Our Approach to Cloud Provider Selection	5
4.1 Choice of Data Catalogue	5
4.2 Technical Architecture Design	6
4.3 European Cloud Provider Criteria	7
5. Assessment	11
5.1 OVHCloud	11
5.2 Scaleway	12
5.3 STACKIT	13
5.4 T Cloud Public	14
5.5 UpCloud	15
6. Practical Comparison	17
6.1 T Cloud Public	17
6.2 Scaleway	17
7. Conclusion	18

1. Why Data Sovereignty Matters Now

Many organisations assume that data is automatically "European" once it is stored in a European data centre. That assumption is not always correct, and its consequences are becoming increasingly tangible.

The US CLOUD Act obliges American technology companies to hand over data upon request to US authorities, regardless of where that data is physically stored. For example, a server in Amsterdam running on infrastructure of an American company still falls under foreign jurisdiction. European legislation does not provide adequate protection in this regard.

For public institutions, healthcare organisations and companies working with sensitive personal data, this is more than a legal matter. It directly impacts GDPR compliance, transparency towards data subjects and reputational risks in case of incidents.

Data sovereignty is therefore not a technical detail, but a strategic choice: deliberately choosing infrastructure and jurisdiction over which the organisation has actual control. This increases legal certainty, reduces dependency on parties outside the EU and strengthens the negotiating position regarding contracts and incidents.

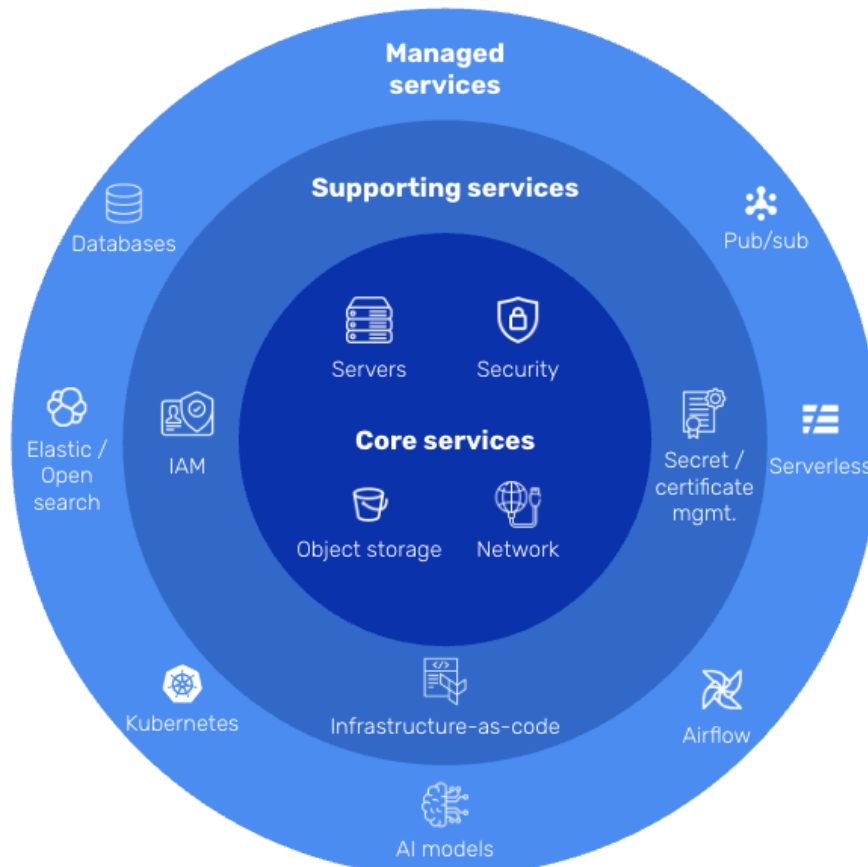
2. The Compared Cloud Providers

For this research, we compared five European cloud providers:

- **OVHcloud** is one of the largest and most established European cloud providers, founded in France in 1999. The company operates data centres spread across Europe and beyond, and offers a broad portfolio from servers to managed services.
- **Scaleway** is a French cloud provider and part of the Iliad Group, founded in 1999. The company focuses on developer-friendly solutions with an emphasis on open standards, transparency and sustainability. Scaleway has data centres in the Netherlands (Amsterdam), France and Poland.
- **STACKIT**, founded in 2018, is the cloud platform of the Schwarz Gruppe, the parent company of Lidl and Kaufland. The provider targets European companies that value data security and control, primarily in Germany, Austria and Switzerland.
- **T Cloud Public (TCP)**, formerly Open Telekom Cloud, is the public cloud solution of Deutsche Telekom. It was founded in 2016 and is one of the largest telecommunications companies in Europe. The provider primarily targets government organisations and large enterprises with high security and compliance requirements.
- **UpCloud** is a Finnish cloud provider, founded in 2012, with a focus on high performance and predictable pricing. The company primarily targets developers and growing organisations and distinguishes itself with a customer-oriented approach. UpCloud is smaller than the other providers in this overview, but operates fully independently and within European jurisdiction.

3. Cloud Provider Maturity

The most important development in the European cloud market is not in basic infrastructure, but in the number and maturity of managed services. American parties offer many open-source software solutions as a managed service, while with European parties you often have to set up and maintain these yourself. The new players in the European market typically have one of two origins: hosting companies or telecommunications companies. The image below shows that cloud providers roughly consist of three layers that together determine how “mature” they are.



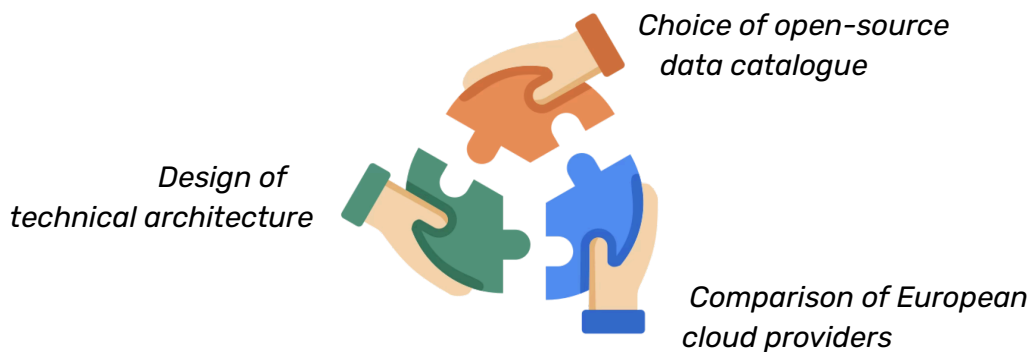
Core Services such as servers, security, object storage and networking. The foundation on which virtually every provider in our comparison now scores well.

Supporting Services such as Identity & Access Management (IAM), secret and certificate management and Infrastructure-as-Code: this layer often makes the difference in practice, because governance, automation and manageability converge here.

Managed Services such as databases, OpenSearch / Elasticsearch, Kubernetes, AI models, applications like Airflow, serverless capabilities and pub/sub. In this area, hyperscalers often lead the way by offering deeply integrated services that are immediately deployable without complex installation or management.

4. Our Approach to Cloud Provider Selection

The selection of a European cloud provider should not be approached as an isolated decision, but as an integral part of a coherent target architecture. Therefore, for the Municipality of Nijmegen, the choice of an open-source data catalogue, the technical design of the data platform and the choice of European cloud provider were all determined in the first phase of the project. Like puzzle pieces, they need to fit together.



We describe the following in sequence:

1. The choice of an open-source data catalogue
2. The technical architecture design
3. The selection criteria for European cloud providers

4.1 Choice of Data Catalogue

The Municipality of Nijmegen had set the explicit requirement that the data catalogue must be based on open-source software. Moreover, the catalogue must integrate well with the other data applications within the platform.

In addition, the Municipality of Nijmegen formulated a number of functional requirements for the data catalogue. The most important functionality of a data catalogue is making the available data easily searchable, including a business glossary. The catalogue must support data lineage visibility, so that the origin and dependencies of datasets are made transparent. The data schema must also be visible down to column level, including associated metadata. Furthermore, the catalogue is expected to facilitate basic data quality checks and enable monitoring of KPIs related to metadata quality. For security purposes, it is important that authentication is handled through SSO.

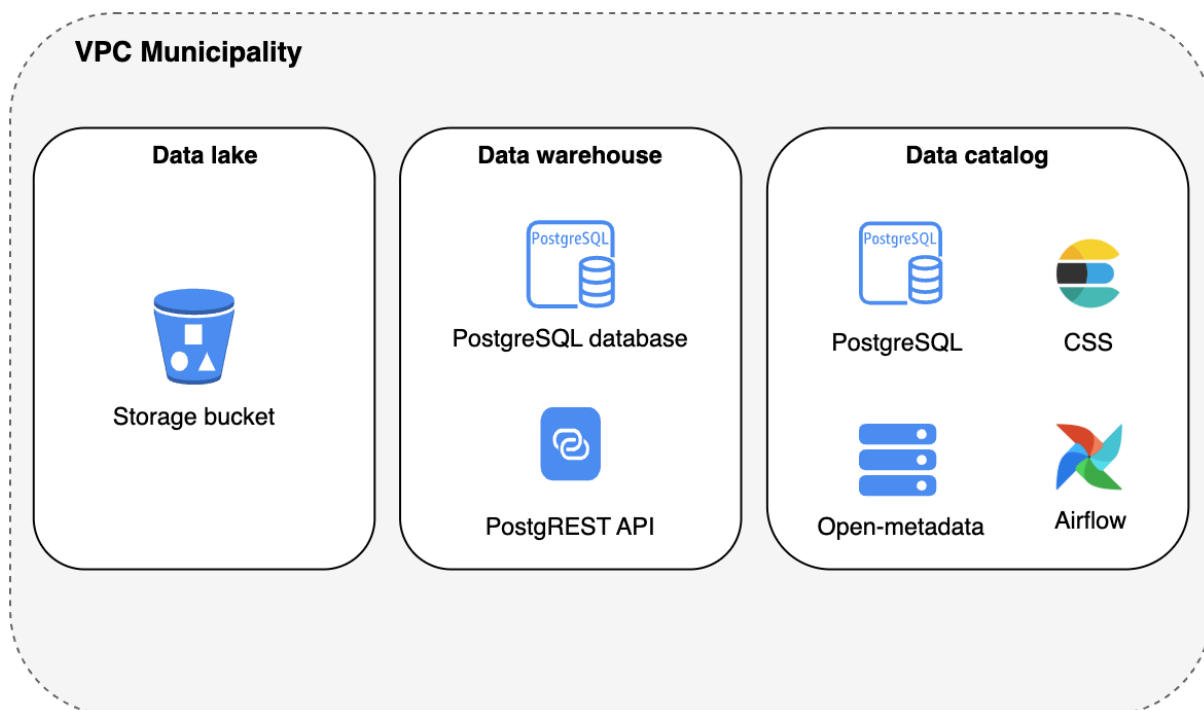
Within this framework, together with the Municipality of Nijmegen, we chose OpenMetadata as the data catalogue. OpenMetadata can be set up in a fully self-managed manner. This prevents dependency on external SaaS services, which often run on American infrastructure, and ensures that metadata and governance settings remain within the organisation's own infrastructure. The choice of OpenMetadata therefore reinforces the objective of data sovereignty and aligns with the principles also applied in the cloud selection.

4.2 Technical Architecture Design

The choice of a European cloud provider cannot be seen separately from the technical architecture that the cloud provider must be able to support. With the requirements specification and the choice of data catalogue, we created an architecture diagram of all required components to roll out the infrastructure.

The goal is to also easily deploy the architecture to additional municipalities. For this, we used a hub-and-spoke model. In this model, a shared VPC serves as the central hub. This is where the private connection from the on-premise environment enters through a central gateway. From this hub, network traffic is distributed across the connected municipalities (the spokes). Each municipality receives a development, acceptance and production version of the infrastructure.

The image below shows the components for a single environment of a municipality.



There is a data lake based on S3-compatible object storage, a (managed) PostgreSQL database serving as a data warehouse with a virtual machine (VM) on which PostgREST enables access to the data warehouse via an API. Finally, there is the data catalogue, which requires four underlying components: (1) PostgreSQL database for metadata, (2) Cloud Search Service (CSS), based on OpenSearch, (3) VM with OpenMetadata and (4) VM with Airflow.

The key design principles we adhered to are:

- Separated environments (development/acceptance/production)
- Infrastructure-as-Code (using Terraform) for reproducibility
- Managed services where possible
- Leveraging existing logging and monitoring of the Municipality of Nijmegen

4.3 European Cloud Provider Criteria

A cloud selection requires more than comparing features in a spreadsheet. Especially when sovereignty, jurisdiction and governance play a role, a structured and well-founded approach is essential. Therefore, we compare European cloud providers based on predefined criteria, considering both legal and technical aspects.

This methodical comparison creates a transparent and reproducible assessment framework, making it explicitly visible where providers differ from each other and which best align with the stated requirements.

In consultation with the Municipality of Nijmegen, the selected providers were assessed based on five interrelated themes: (1) General, (2) Security, (3) Services, (4) Cost and (5) Support and willingness to invest. The assessment was conducted on 15 October 2025. Since the European cloud market is evolving rapidly and providers continuously expand and adjust their service portfolio, this assessment represents a point-in-time snapshot. The five themes are explained below.

4.3.1 General

The general criteria provide insight into the background and positioning of the cloud provider. They address aspects such as data sovereignty, transparency, sustainability and strategic direction. These factors determine the extent to which a provider fits within European and organisational values and provide context for the technical and operational choices.

- **Data Sovereignty**
Assesses the extent to which the provider meets European data sovereignty requirements, including ownership and management of data centres within the EU and protection against foreign legislation such as the US CLOUD Act. Also considers the degree of operational control that customers have over their own environments.
- **Sub-processors**
Concerns the transparency with which the provider provides insight into the sub-processors used, their role and location. Important here is whether customers can easily verify where data is processed and under which jurisdiction.
- **Availability Zones**
Measures the geographical spread and redundancy of data centres within a region, and the extent to which this contributes to the continuity and fault tolerance of services.
- **Environment**
Assesses the provider's sustainability efforts, including energy efficiency, use of renewable energy, circular hardware and broader CSR initiatives such as diversity and community engagement.
- **CSR (Corporate Social Responsibility)**
Examines the social responsibility of the provider, including ethical business practices, social impact and initiatives in sustainability and inclusivity.
- **Roadmap**
Evaluates the availability and transparency of the public product roadmap, the

frequency of innovations and the extent to which the provider invests in further platform development.

4.3.2 Security

The security criteria focus on the safeguards a provider offers to protect data and infrastructure. They encompass both formal certifications and practical measures, such as conducting penetration tests and adhering to international standards.

- **ISO27001**

Verifies whether the provider is certified according to the ISO 27001 standard for information security and whether the certificate is current and applicable to the services used. This is to validate that the solution will comply with the Baseline Information Security Government (BIO2).

- **Penetration Tests**

Assessment of whether customers receive permission and support to conduct their own penetration tests on their cloud environments, including any restrictions or approval procedures.

4.3.3 Services

This category assesses the functional richness and technical maturity of the platform. This includes the availability of managed services, the quality of database and storage solutions, network options, access management and capabilities for automation and integration.

- **Managed Services Availability**

Examines which managed services the provider offers (such as databases, object storage, API management) and how mature and stable these services are. Evaluates the availability of automatic backups and Point-in-Time Recovery (PITR), including retention periods and recovery options.

- **PostgreSQL**

Addresses the availability and quality of a managed PostgreSQL service, including configuration options, performance and maintenance. In this section, we also assess the availability of additional PostgreSQL extensions such as PostGIS and PostgREST.

- **OpenSearch / Elasticsearch**

Addresses the availability and quality of a managed OpenSearch or Elasticsearch service. These are required for most data catalogues.

- **S3-compatible object storage**

Evaluates whether the provider offers object storage with an S3-compatible API and the extent to which it is fully interoperable with existing S3 tools and SDKs.

- **Logging**

Examines the extent to which logging and auditing of activities is possible, and whether these logs are centrally accessible and exportable.

- **Private Connections**

Assesses the availability of direct network connections (such as Direct Connect or ExpressRoute) for secure and performant links with on-premise infrastructure. VPN tunnels are considered a less optimal alternative.

- **API Managed Service**

Specifically focuses on the ability to use PostgREST or similar services as a managed API layer on top of Database-as-a-Service (DBaaS).

- **API Resource Access**

Measures the extent to which resources within the cloud platform are accessible and manageable via APIs, for example for provisioning, monitoring and automation.

- **IAM (Identity and Access Management)**

Assesses the granularity and maturity of access management within the cloud platform and object storage. Important here is how fine-grained permissions can be assigned and managed. Also examines the capabilities for provisioning users and accounts within the data platform, including central management capabilities, roles and permission structures.

- **Entra ID Integration**

Covers two aspects: the ability to use Entra ID (formerly Azure AD) to sign in to the cloud platform, and to link role-based access control (RBAC) in managed PostgreSQL to Entra ID users and groups.

- **Infrastructure-as-Code**

Assesses the support for Infrastructure-as-Code (IaC) via Terraform, including the completeness of API coverage and documentation.

4.3.4 Cost

The cost criteria provide insight into the transparency and predictability of pricing models. They cover topics such as data traffic (egress and ingress), billing options and the financial structure of the billing model. In the preliminary phase, a comparison had already been made of the major players and the costs for consuming servers and services. The conclusion was that costs differ only marginally between providers and would therefore not be decisive in the choice.

- **Egress**

Measures the costs for outbound data traffic, often a significant factor in the total usage costs of cloud environments.

- **Ingress**

Assesses whether inbound data traffic is free of charge or offered at a reduced rate.

- **Direct Billing Available**

Determines whether customers can settle directly with the provider without intermediation by resellers or partners, and which billing options are available.

4.3.5 Support and Willingness to Invest

This category assesses the quality of support and the extent to which a provider invests in customer relationships and platform development. Topics such as support levels, expertise, documentation and availability of resources provide a picture of the organisation's engagement and maturity.

- **Support Levels**

Evaluates the available support levels (e.g. standard, premium) and associated response times and Service Level Agreements (SLAs). This also includes the completeness, currency and quality of the technical documentation.

- **Subject Matter Expertise**

Assesses the technical expertise of support staff and the availability of specialised engineers or consultants.

- **Language**

Indicates in which languages support and documentation are available, with emphasis on support in English and possibly local languages.

Each criterion is rated on a scale of 1 to 3, depending on its relative importance to the organisation. Subsequently, a substantive assessment is given per cloud provider, including an explanation. A visual indication is used: green for suitable or fully supporting, amber for partially suitable or point of attention, and red for insufficiently suitable within the stated requirements.

5. Assessment

5.1 OVHCloud

Theme	Criteria	Rating	Explanation
General	Sovereignty		Sovereign, though they do have a co-location in Italy where the building is not their property.
	Sub-processors		Uses a sub-processor for the most critical part of the architecture: managed PostgreSQL.
	Availability Zones		They offer 3 AZs in the Paris region.
	Environment		PUE 1.26, figures from 2022, 92% renewable: https://corporate.ovhcloud.com/nl/sustainability/environment/
	CSR		They have CSR policies in place.
	Roadmap		Public roadmap: https://github.com/orgs/ovh/projects/16
Security	ISO27001		Certifications and reports for ISO/IEC 27001, 27017 and 27018.
	Penetration tests		Permitted without prior coordination, which raises questions.
Services	Managed Services Availability		All services are available as managed, except for Airflow.
	PostgreSQL		Uses sub-processor Aiven, OIDC not available.
	S3-compatible object storage		Offered by OVH.
	OpenSearch / ElasticSearch		OpenSearch available.
	Logging		Logs Data Platform available for central logging.
	Private Connections		VPN and Direct Connect available.
	API Resource Access		Resources can be accessed via the API.
	IAM and Account Management		Granularity of configurable IAM is limited.
	Entra ID Integration		OIDC not available in PostgreSQL.
	Infrastructure-as-code		Role management via IaC is limited.
Cost	Egress		Free egress, except for S3.
	Ingress		Free ingress.
	Direct Billing Available?		This is available.
Support	Support Levels		For more technical questions, you are immediately referred to Professional Services (€+).
	Subject Matter Expertise		Disadvantage that substantive questions about managed PostgreSQL must go to Aiven. Professional services are also quickly needed here.
	Language		EN / DE

5.2 Scaleway

Theme	Criteria	Rating	Explanation
General	Sovereignty		Sovereign, but only operate co-locations.
	Sub-processors		Extensive use of co-locations managed by sub-processors: Equinix, Iron Mountain, Digital Realty.
	Availability Zones		Scaleway has a multi Availability Zone in Northern Europe, including two data centres in Amsterdam. Additionally, (co-)locations in Poland and France, among others.
	Environment		PUE 1.37, 100% renewable: https://www.open-telekom-cloud.com/en/benefits/sustainability
	CSR		They have CSR policies in place.
	Roadmap		No public roadmap.
Security	ISO27001		Available: https://www.scaleway.com/en/security-and-resilience/
	Penetration tests		Permitted under conditions
Services	Managed Services Availability		All services are available except for Airflow. Many in beta, and therefore only available in Paris.
	PostgreSQL		PostGIS available. However, PostgREST is not available.
	S3-compatible object storage		Offered by Scaleway.
	OpenSearch / ElasticSearch		OpenSearch in beta only.
	Logging		Logging not offered as a separate service, but a central dashboard is available.
	Private Connections		Tunnel available, but from the REST API for partners, no partner appears to be available for AMS
	API Resource Access		Resources can be accessed via the API.
	IAM and Account Management		Granularity of configurable IAM is limited.
	Entra ID Integration		Entra ID integration is available.
	Infrastructure-as-code		Beta services not available in Terraform provider. Documentation is limited.
Cost	Egress		Free egress, except for S3.
	Ingress		Free ingress.
	Direct Billing Available?		This is available.
Support			
	Support Levels		No SLA for beta services. Certification required above a certain service level.
	Subject Matter Expertise		Appears adequate after initial meetings, strong willingness to collaborate.
	Language		FR / EN, occasionally French is still found on the website and in documentation.

5.3 STACKIT

Theme	Criteria	Rating	Explanation
General	Sovereignty		Sovereign, with own locations.
	Sub-processors		No sub-processors.
	Availability Zones		They offer multi-AZ in Germany.
	Environment		PUE 1.1 - 1.5, reported somewhat ambiguously, 100% renewable: https://www.stackit.de/en/knowledge/sustainability-cloud/
	CSR		They have CSR policies in place.
	Roadmap		No public roadmap
	ISO27001		Available: https://www.stackit.de/en/colocation/
Security	Penetration tests		Possible upon consultation.
Services	Managed Services Availability		More server-focused, fewer services available. All required services are available except for Airflow (expected end of 2025).
	PostgreSQL		PostGIS not available as an extension in managed service.
	S3-compatible object storage		Offered by STACKIT.
	OpenSearch / ElasticSearch		OpenSearch available.
	Logging		LogMe and Observability managed services available
	Private Connections		No tunnel or direct connect available. VPN in beta.
	API Resource Access		Resources can be accessed via the API.
	IAM and Account Management		IDP limited, no custom roles,
	Entra ID Integration		Entra ID integration is not available.
	Infrastructure-as-code		Terraform support is very limited.
Cost	Egress		Free egress, except for S3.
	Ingress		Free ingress.
	Direct Billing Available?		This is available.
Support	Support Levels		Takes long to get an appointment. Phone number on website not in use. Documentation is very sparse.
	Subject Matter Expertise		Appears adequate after initial meetings.
	Language		DE / EN

5.4 T Cloud Public

Theme	Criteria	Rating	Explanation
General	Sovereignty		Sovereign, fully owned locations.
	Sub-processors		Does not use sub-processors other than sister company Deutsche Telekom.
	Availability Zones		Has 3 availability zones in the Netherlands.
	Environment		PUE 1.28, 100% renewable: https://www.open-telekom-cloud.com/en/benefits/sustainability
	CSR		They have CSR policies in place.
	Roadmap		Public roadmap: https://www.open-telekom-cloud.com/en/products-services/roadmap
Security	ISO27001		Certifications: https://www.open-telekom-cloud.com/en/products-services/core-services/certifications
	Penetration tests		Prior approval must be requested.
Services	Managed Services Availability		All services are available as managed, except for Airflow. Key management in beta.
	PostgreSQL		PostGIS and OIDC available. However, PostgREST is not available.
	S3-compatible object storage		Offered by TCP.
	OpenSearch / ElasticSearch		OpenSearch available.
	Logging		Log Tank Service available for central logging.
	Private Connections		VPN and Direct Connect available.
	API Resource Access		Resources can be accessed via the API.
	IAM and Account Management		TCP has the most detailed IAM implementation of all providers, comparable to AWS.
	Entra ID Integration		Entra ID integration is available.
	Infrastructure-as-code		Very well-documented Terraform provider + broad coverage incl. IAM.
Cost	Egress		Paid egress, the only one of the 5 providers.
	Ingress		Free ingress.
	Direct Billing Available?		This is available.
Support	Support Levels		24/7 telephone support available in English. Extensive online documentation available.
	Subject Matter Expertise		Appears adequate after initial meetings.
	Language		EN / DE, also have support in the Netherlands due to other major clients.

5.5 UpCloud

Theme	Criteria	Rating	Explanation
General	Sovereignty		Sovereign, with own locations.
	Sub-processors		No sub-processors.
	Availability Zones		UpCloud has multi-AZ in fi-hel or via enterprise private cloud.
	Environment		PUE not published, 70% renewable: https://upcloud.com/esg-report-2024/
	CSR		They have CSR policies in place.
	Roadmap		No public roadmap.
Security	ISO27001		Available: https://upcloud.com/security-privacy/
	Penetration tests		24h advance notice required.
Services	Managed Services Availability		More server-focused, fewer services available. All required services are available except for Airflow and logging.
	PostgreSQL		PostGIS available. However, PostgREST is not available.
	S3-compatible object storage		Offered by UpCloud.
	OpenSearch / ElasticSearch		OpenSearch available.
	Logging		Logging not offered as a separate service.
	Private Connections		Tunnel available, no direct connect.
	API Resource Access		Resources can be accessed via the API.
	IAM and Account Management		Granularity of configurable IAM is very limited.
	Entra ID Integration		Entra ID integration is not available.
	Infrastructure-as-code		Terraform support is very limited.
Cost	Egress		Free egress.
	Ingress		Free ingress.
	Direct Billing Available?		This is available.
Support	Support Levels		It is noticeable that this provider is still young and less developed than the competitors.
	Subject Matter Expertise		Appears adequate after initial meetings, strong willingness to collaborate.
	Language		English.

Below, the results are consolidated in a single overview. This overview enables a direct comparison of the cloud providers and provides a summary picture of how the different European providers compare to each other.

Theme	Criteria	#	OVHCloud	Scaleway	StackIT	TCP	UpCloud
General	Sovereignty	3					
	Sub-processors	2					
	Availability Zones	2					
	Environment	2					
	CSR	2					
	Roadmap	1					
Security	ISO27001	2					
	Penetration tests	2					
Services	Managed Services Availability	3					
	PostgreSQL	3					
	S3-compatible object storage	3					
	OpenSearch / Elasticsearch	2					
	Logging	2					
	Private Connections	3					
	API Resource Access	2					
	IAM and Account Management	2					
	Entra ID Integration	2					
	Infrastructure-as-code	3					
Cost	Egress	1					
	Ingress	1					
	Direct Billing Available	2					
Support	Support Levels	3					
	Subject Matter Expertise	2					
	Language	2					

In this case, TCP distinguishes itself by offering the most mature services, without using sub-processors. The maturity of the services becomes particularly evident in supporting services such as IAM and Microsoft Entra ID integration (a requirement of the Municipality of Nijmegen). Their data centres use 100% renewable energy and they additionally offer private connect solutions and the ability to apply Infrastructure-as-Code.

However, a cloud provider can meet all requirements on paper, while in practice limitations may still become apparent. Therefore, the selection is only finalised once the architecture has actually been tested and conversations have been held with various cloud providers.

6. Practical Comparison

Based on the substantive assessment, TCP and Scaleway emerged as the most suitable candidates. To obtain a complete picture, both providers were also practically validated by actually building a proof-of-concept environment.

6.1 T Cloud Public

Setting up services via the management console runs smoothly and aligns well with the stated requirements. However, bottlenecks arose when using the CLI. Documentation is sometimes split between TCP's own documentation and the underlying OpenStack documentation, with discrepancies that cause confusion. Additionally, the software dependencies per version of the CLI tooling are not always clearly documented, which requires additional investigation.

Furthermore, HashiCorp provides support for an S3-compatible Terraform Backend for TCP only on a *best effort*. Due to a recent version update, it is no longer possible to use a secrets manager for this configuration. Workarounds are available, but this requires extra attention during implementation.

6.2 Scaleway

The willingness to collaborate and the quality of support during the exploratory meetings were convincing enough to also practically validate Scaleway. However, that practical test ran into fundamental limitations around Infrastructure-as-Code early on.

For instance, the management of Identity and Access Management (IAM) is still under active development: configuring security groups via Terraform is currently not possible. More broadly, all services still in beta – a significant portion of the required portfolio – are not available within the Terraform provider. For a production environment that must be built on automated, repeatable infrastructure, this is an insurmountable obstacle.

Despite the better support experience, Scaleway therefore does not meet the stated requirements and is unsuitable as a foundation for the data platform.

Lessons from Practice

The practical experience confirms a pattern that is often visible in cloud comparisons: the differentiator is rarely in the basic provisions. Serious providers offer compute, storage and networking at a comparable level. The real differences become visible in the layer surrounding them.

Access management is the first indicator in this regard. The extent to which permissions can be assigned in a fine-grained manner, integrated with existing identity systems and fully auditable, largely determines whether a platform is suitable for organisations with strict governance requirements.

Maturity of managed services is the second. Databases, Kubernetes platforms and monitoring services exist at virtually every provider, but stability, documentation and manageability vary significantly. What matters is not the number of available features, but the extent to which services function consistently and predictably in a production environment.

Integration is the third and most distinguishing factor. A standalone database or storage service is rarely the bottleneck. The decisive question is how components work together within the broader ecosystem of identity, logging, networking and automation. It is precisely in this coherence (or the lack thereof) that it becomes visible whether a cloud platform is truly mature.

Finally, data sovereignty requires more than a contractual agreement. Legal control must be supported by deliberate architecture choices: transparency about sub-processors, a consistent design of access management and infrastructure that can be overseen and accounted for as a whole. Only when technology and governance reinforce each other does actual control over the digital foundation emerge.

7. Conclusion

The European cloud market now offers alternatives to hyperscalers. The decisive factor is not in the availability of basic services, but in legal control, identity & access management, integration and the maturity of managed services.

Based on the inventory of cloud providers and the practical experience we gained, we advised the Municipality of Nijmegen to choose **T Cloud Public (TCP)** to build their data platform on.

The comparison of different European cloud providers shows that the market is developing at a rapid pace. Features that are currently limited or absent can become available within a few months. For example, at cloud provider STACKIT, support for specific PostgreSQL extensions such as PostGIS was initially not offered, and we also reported this in our discussions. This has since been resolved and is now available. Therefore, we actively follow developments and continue to assess whether choices still align with the strategic objectives of the municipality. After all, choosing a cloud provider is not a point-in-time decision, but a strategic decision with long-term impact.

Questions? Or would you like to explore which European cloud provider best fits your organisation? We are happy to assist with selection, architecture and implementation.