

Public cloud from Europe

Even though most people think of US hyperscalers when they hear the word "cloud," European providers have long been competitive in many areas. European clouds are an important building block for greater digital sovereignty.

By Prof. Dr. Jens-Henrik Söldner,
Dr Constantin Söldner and Dr Guido-Arndt Söldner



■ Since cloud computing made its breakthrough in the 2010s, there has been a desire in the European Union to create a secure, data-sovereign cloud infrastructure for Europe. The current uncertain geopolitical situation and growing regulatory requirements have led to a stronger focus on European cloud providers. However, if you look at their market share, it quickly becomes clear that American cloud providers clearly dominate the field. European providers are growing, but their market share in the European market remains small.

According to Christian Scholz, Vice President Cloud Business at Arvato Systems, however, more than individual initiatives are now needed, as no single provider in Europe has the financial resources to seriously compete with the US tech giants on all levels. Rather, cooperation between the state and industry is needed

in order to build internationally competitive European cloud competitors in the coming years. One such cross-sector initiative is the Sovereign Cloud Stack (SCS) – an open-source-based cloud and container platform that serves as the technical foundation for the European cloud project Gaia-X and is supported by companies such as Telekom, plusserver, noris network, B1 Systems and several others.

Factors influencing the choice of cloud

This raises the question for many IT managers as to which of their use cases European providers can already offer an adequate alternative to the seemingly overpowering American providers. To answer this question, you need a list of criteria relevant to your own use case. One of the most important factors is the scope of the cloud services offered and

services in the areas of computing, networking and storage, many companies are interested in PaaS (Platform as a Service) services such as managed databases or container orchestration platforms such as Kubernetes.

Another criterion is the geographical availability of the respective cloud provider. While large hyperscalers such as AWS, Azure and Google have global data centres in all major hotspots, smaller providers are more geographically limited or focus on specific target markets. In this context, decision-makers should also consider the number of data centres in a given region. This not only determines availability, but is also important for scalability: even large hyperscalers cannot grow indefinitely, as in some regions the power grid simply cannot support further growth. Customers may therefore have to switch to other regions.

In addition to technical factors, costs play a significant role. Companies have already realised that simple lift and shift, i.e. moving workloads to the cloud without changing the architecture, does not take advantage of the benefits of the cloud and is usually more expensive. When it comes to running virtual machines, traditional hosters are often unbeatably cheap. On the other hand, the large hyperscalers offer pricing models in which customers benefit from significant discounts for longer-term commitments.

ABSTRACT

- European cloud providers already offer comprehensive IaaS services in the areas of computing, storage and networking. However, they still have some catching up to do in terms of managed services and specialised functions compared to the US hyperscalers AWS, Azure and Google Cloud.
- As European companies, they are subject to European law, which ensures compliance with regulations such as the GDPR.
- The market shares of European providers are still small, but are growing, as is the number of services offered.

can benefit from significant discounts. It is therefore essential to take a closer look at the providers' pricing models.

Compliance and technology

An increasingly important factor for Dutch and European customers is compliance with regulatory requirements, particularly data sovereignty. In addition to the General Data Protection Regulation (GDPR), which governs the processing of personal data, there are industry-specific EU regulations such as DORA and NIS2. National regulations such as the KRITIS Regulation for critical infrastructure also play a role. Cloud providers must increasingly demonstrate compliance with these regulations, but also provide their customers with services that enable them to comply with these requirements.

In order to compare the various European cloud providers, it is necessary to understand the key features of a public cloud. In addition to the availability of data centres, these include features in the three classic areas of compute, network and storage (IaaS). Furthermore, the PaaS offering (e.g. databases, Kubernetes, etc.) of the manufacturers plays a major role. Management services must be available and automation must be in place to operate the cloud. possible. A not insignificant role Security features and functions that enable users to secure their cloud environments also play a role.

Physical infrastructure

Running applications in the cloud requires a minimum number of data centres in one or more geographical regions to ensure the availability and reliability of the applications. The provider does not have to operate the data centre itself; it can also rent space in existing data centres. Even the large hyperscalers still rely on other data centre providers when establishing new regions. Customers are increasingly demanding physical redundancy of at least two data centres in order to meet the high availability and thus the SLAs of their applications. For globally active companies, a presence in the major economic areas is also necessary. Furthermore, it is advantageous for customers if providers have their own

Produkte & Cloud Services			
https://www.open-telekom-cloud.com/de/produkte-services/core-services			
Open Telekom Cloud Produkte Preise Lösungen Partner Academy Marketplace Support News Suche Login			
Computing	Region DE	Region NL	
Auto Scaling	✓	✓	①
Bare Metal Server	✓	--	①
Dedicated Host	✓	✓	①
Elastic Cloud Server	✓	✓	①
FunctionGraph	✓	--	①
Image Management Service	✓	✓	①
Container	Region DE	Region NL	
Application Service Mesh	✓	--	①
Cloud Container Engine	✓	✓	①
Cloud Container Instance	✓	--	①
Software Repository for Container	✓	✓	①
Speicher	Region DE	Region NL	
Cloud Backup and Recovery	✓	✓	①
Cloud Server Backup Service	✓	--	①
Elastic Volume Service	✓	✓	①
Object Storage Service	✓	✓	①
Scalable File Service	✓	✓	①
Storage Disaster Recovery Service	✓	--	①
Volume Backup Service	✓	--	①
Datenbanken	Region DE	Region NL	
Data Replication Service	✓	✓	①
Distributed Cache Service	✓	✓	①
Distributed Database Middleware	✓	--	①
Document Database Service	✓	✓	①
GaussDB (für MySQL)	✓	--	①
GeminiDB	✓	--	①
Oracle-optimized	✓	--	①
Relational Database Service	✓	✓	①
Netzwerk	Region DE	Region NL	
Direct Connect	✓	✓	①
Domain Name Service	✓	✓	①
Datenanalyse	Region DE	Region NL	
Cloud Search Service	✓	✓	①
DataArts Studio	✓	--	①

The Open Telekom Cloud offers a wide range of services. At the bottom right is the smart AI chatbot Cloudia (Fig. 1).

backbone between their various Provide data centres, otherwise they will have to establish VPN connections between the locations. In addition to the actual data centres, some cloud providers offer additional points of presence (PoPs) that do not host any workloads but are physically closer to the customer locations and therefore offer a shorter route to the cloud provider's network. Cloud providers also use such PoPs as content delivery networks (CDNs) for caching website content.

Compute capacity

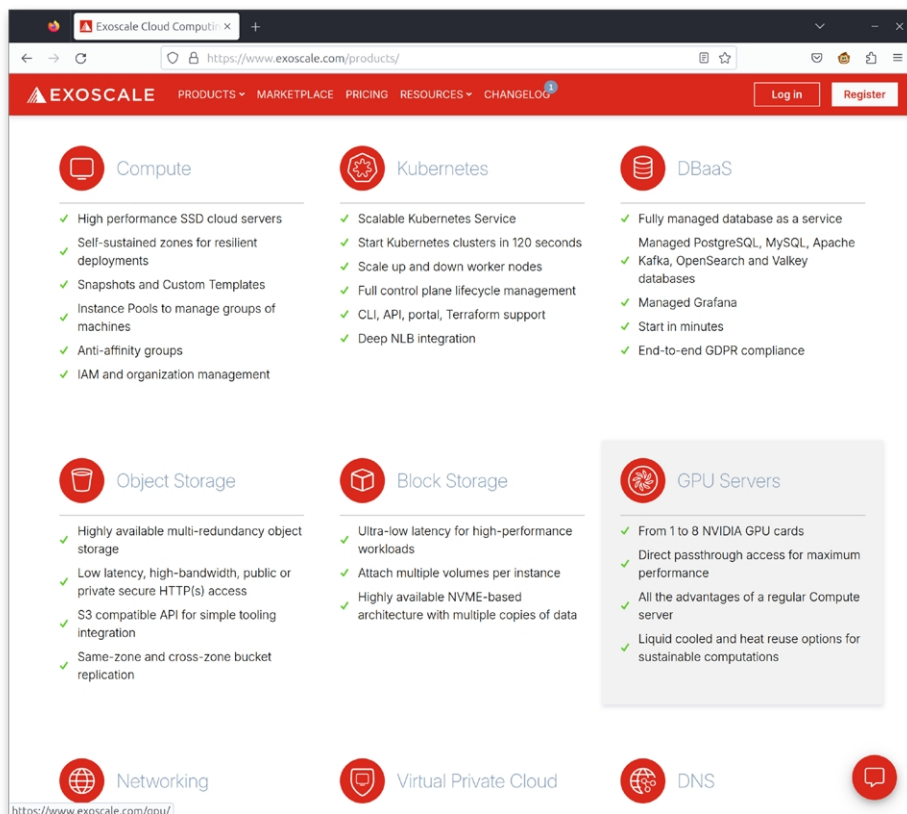
In order to meet the requirements of different workloads, cloud providers must offer a wide range of different hardware configurations and machine sizes. The VM types offered are typically divided into the categories general purpose, CPU-optimised, memory-optimised, storage-optimised and network-optimised. In addition, there is support for specialised hardware such as that used for AI applications.

hardware such as GPUs or FPGAs, which are essential for AI applications . Customers consume these VMs in different "T-shirt sizes" such as S, M, or XL. However, it is not only the bare hardware that is important to customers, but also the range of machine images for the most common operating systems, from Windows Server to various Linux distributions.

A key cost-saving feature for customers, especially for VM-based workloads, is autoscaling, i.e. scaling up and down the number of VMs deployed based on specific metrics such as CPU utilisation. This allows customers to ensure that the necessary capacity is available during peak times, but also to save money when utilisation decreases again.

Storage diversity

Storage is the second essential infrastructure component that cloud providers offer in various forms. To operate virtual machines, customers primarily need



One of Exoscale's focal points is GPU servers (Fig. 2).

Line of classic block storage. In addition magnetic hard drives (HDD), the cloud provider should offer SSD storage in different performance tiers. In addition, many cloud providers offer VMs with local storage, which are designed specifically for running special latency-critical applications with high IOPS requirements.

In addition to the block and file storage commonly used on-premises, object storage is a central cornerstone of the public cloud. This cost-effective, scalable storage, which can be accessed via the HTTP(S) protocol, has a wide range of uses. These include, above all, unstructured data, backup storage, the provision of website data, the storage of log files and even data lakes. Its high availability is also worth highlighting, as the data is usually replicated and stored multiple times in different data centres. Despite these advantages, object storage stands out from other types of storage due to its low price.

Virtual networks

Virtual private clouds (VPCs) are a central element of cloud computing.

AWS introduced VPCs in 2009, with which allow customers to create and customise isolated virtual networks in the cloud. Initially, VPCs offered basic functions such as defining IP address ranges, creating subnets, configuring routing tables, security groups and network ACLs. They offer numerous advantages such as cost efficiency through pay-as-you-go models, scalability, internet access and innovation potential.

This was followed in 2014 by the introduction of VPC peering, which enabled connections between VPCs. In large environments, it can be costly to peer all VPCs with each other and create a mesh architecture. That is why, at the end of the 2010s, offerings such as AWS Transit Gateway came onto the market, making it possible for VPCs to communicate with less effort than with peering.

An encrypted connection between a local network and a VPC is also very important, as it enables secure communication, for example via IPsec or other protocols. Many cloud providers offer this type of function as a managed service; if not, you can always help yourself with a manual setup and configure the VPN yourself for web applications via HTTPs.

install virtual machines. In addition to VPNs, dedicated lines enable dedicated private network connections between local networks and the cloud with high bandwidth, low latency and without using the public internet. Here, too, a number of providers score highly, rivalling the American hyperscalers in terms of functionality and performance.

Virtual machines in VPCs should avoid using public IP addresses wherever possible. For this reason, NAT gateways have become very popular with customers as a managed service since the mid-2010s – if they are not available, they must be operated independently. Load balancers should be used for incoming traffic whenever possible. Depending on the use case, Layer 7 load balancers are usually required for HTTP(S)-based traffic and Layer 4 load balancers for TCP traffic.

Finally, DNS as a managed service is helpful for making offerings accessible via the web. If the offering is to be accessible from the internet, public DNS zones must be set up in the DNS – private zones are required for internal access. To secure web applications via HTTPs Valid certificates are necessary. It is particularly helpful to integrate the load balancer with a certificate authority to generate the certificates. Many providers integrate Let's Encrypt for this purpose.

APIs and automation

In addition to the scope of services offered, broad support for automation solutions is of central importance for cloud computing. The use of CLI tools, APIs and SDKs, as well as infrastructure-as-code tools, not only ensures consistency and repeatability, greater scalability and efficiency, but also reduces errors. GitOps approaches allow for configuration versioning and team collaboration. Meaningful abstraction and provider-independent tools such as Terraform reduce vendor lock-in and enable efficient management of multi-cloud environments. Such tools are also important for security and compliance: GitOps approaches, for example, enable the definition of a secure configuration that can be repeated and audited. Last but not least, the provision of resources can be significantly shortened.

Many cloud providers already offer automation interfaces. For OpenStack-based cloud solutions, the supplied OpenStack interfaces can sometimes also be used, for example the OpenStack Terraform provider in combination with the providers' proprietary providers. However, compared to the American hyperscalers, European offerings currently lag far behind in terms of the scope of automation. This also applies to documentation, where American providers offer a great deal of helpful support.

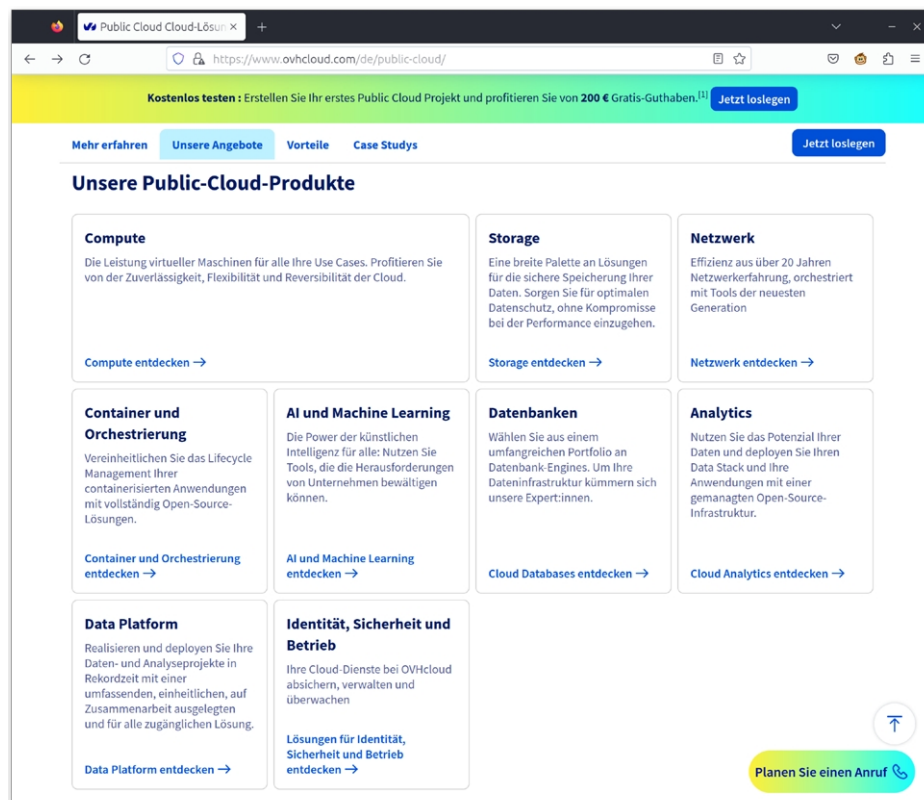
When it comes to Kubernetes automation, however, the difference is much smaller. Once a company has a Kubernetes cluster up and running, it can draw on the wide range of open source solutions offered by the Cloud Native Linux Foundation (CNCF). Here, there are few differences in terms of automation.

PaaS services and managed services

In addition to basic IaaS services, PaaS services such as databases and container platforms are a key reason for running workloads in the cloud. PaaS services are usually available as managed services and are characterised by simplified administration, fast provisioning, scalability and cost efficiency. The MySQL, PostgreSQL and MariaDB databases are part of the standard PaaS offering from cloud providers – Microsoft SQL Server and Oracle are also sometimes available. High availability is important for customers: databases should offer automatic failover across zone boundaries.

Many customers also want container platforms as a PaaS service. Kubernetes has established itself as the standard here in recent years. Since installing and operating a vanilla Kubernetes environment or a Kubernetes distribution requires a certain amount of effort, Kubernetes as a managed service is now one of the most popular services in public cloud computing.

For many use cases, Kubernetes is oversized, especially if only a few or simple web applications are to be operated. In these cases, a simpler



OVH operates its cloud data centres in nine countries (Fig. 3).

useful container platform such as Cloud Foundry.

Cloud management

To keep track of their workloads in the cloud, companies need tools to manage their environment. These include monitoring tools that evaluate and visualise metrics, logs and, in some cases, traces. Since many companies use third-party monitoring tools, there should be a way to export this data. In addition, customers benefit from tools that provide recommendations for optimising their workloads, for example for rightsizing virtual machines or identifying unused resources.

In principle, companies must be able to transparently track the costs incurred through the use of the cloud. It is common practice for customers to be able to analyse costs in a dashboard according to various dimensions, such as service, resource, region or tags. Here, too, a fine-grained export of all costs incurred for analysis with third-party tools is helpful.

Another issue that is essential for operations is the backup of cloud workloads.

This is handled either by the cloud provider's own backup services or by third-party tools, for which the provider must then provide interfaces. For example, cloud providers typically offer the option of creating snapshots of virtual hard disks to back up VMs.

Who is responsible for security?

There is hardly any topic that is as critical for cloud customers as the security of their applications. Typically, security in the cloud is understood as a shared responsibility, with providers responsible for the security of the cloud and customers responsible for security within the cloud. A fundamental building block is robust identity and access management (IAM) with options for securing identities and assigning rights with role-based access control (RBAC). Multi-factor authentication and conditional access are particularly important for securing identities. In addition, many customers want to be able to import existing identities, for example from their Active Directory, into the cloud's IAM and authenticate users via SSO.

Public cloud providers from Europe

	Exoscale	Hetzner	IONOS	Open Telekom Cloud	OVHcloud	plusserver	Scaleway	STACKIT
Company headquarters	Switzerland	Germany	Germany	Germany	France	Germany	France	Germany
Availability zones	☑	–	☑	☑	☑	☑	☑	☑
VM autoscaling	☑	–	☑	☑	☑	–	☑	–
Object Storage	☑	☑	☑	☑	☑	☑	☑	☑
File Storage	–	–	☑	☑	☑	☑	–	–
Virtual Private Cloud (VPC)	☑	☑	☑	☑	☑	☑	☑	☑
Peering between VPCs	☑	–	–	☑	☑	–	☑	☑
Managed VPN	–	–	☑	☑	☑	☑	–	☑
Dedicated private network connection	–	–	☑	☑	☑	☑	–	☑
Transit gateway	–	–	–	☑	☑	–	–	–
Managed NAT	–	–	–	☑	–	☑	☑	☑
Managed Load Balancer	☑	☑	☑	☑	☑	☑	☑	☑
DNS	☑	☑	☑	☑	☑	☑	☑	☑
SSL Certificate Management	☑	☑	☑	☑	☑	☑	☑	☑
Terraform	☑	☑	☑	☑	☑	☑	☑	☑
Serverless computing	–	–	–	☑	–	–	☑	–
Managed Kubernetes	☑	☑	☑	☑	☑	☑	☑	☑
Managed Databases	☑	–	☑	☑	☑	☑	☑	☑
Metrics/Logs	☑/☑	☑/–	☑/☑	☑/☑	☑/☑	☑/☑	☑/☑	☑/☑
Backup service	☑	☑	☑	☑	☑	☑	☑	☑
Encryption with customer-managed keys (CMK)	☑	–	☑	☑	☑	–	☑	–
Import of external identities (e.g. from Microsoft AD) / SSO	☑	–	☑	☑	☑	–	–	–
BSI-C5 certification	–	–	Type I	Type II	–	Type II	–	Type I

Audit logs are essential for traceability and security monitoring. Companies want to be able to track all login attempts and API operations within their cloud environment. In addition, cloud providers should also offer the option to export these logs.

Another important issue is data encryption. Although most cloud providers already encrypt data by default, it is often necessary, not least from a compliance perspective, for customers to retain control over the encryption keys used (customer-managed keys).

The European perspective

Below and in the table, we present a selection of European public cloud providers – by no means exhaustive – with a focus on larger companies offering a comparatively wide range of services. All of the providers listed are subject to European law, which guarantees compliance with the GDPR as well as other European regulations from NIS2 to the AI Act.

European regulations from NIS2 to the AI Act.

Exoscale

The Swiss cloud provider Exoscale is a subsidiary of the Austrian company A1 Telekom Austria, with two data centres each in Switzerland, Austria and Germany, and one data centre in Bulgaria. The range of services includes IaaS services for compute, networking and storage, as well as managed services for relational and NoSQL databases and Kubernetes, among other things. Another focus is on GPU instances for AI applications.

Hetzner Cloud

Hetzner Cloud operates three data centres in Europe, two of which are in Germany (Falkenstein and Nuremberg) and one in Helsinki. It also has two data centres in the USA and one in Singapore. One of the strongest arguments in favour of Hetzner Cloud is its excellent price-performance ratio. The focus is strongly on infrastructure.

as a Service such as virtual machines, object storage or load balancers. Hetzner has hardly offered Platform as a Service to date.

IONOS Cloud

IONOS, part of the United Internet Group, was founded in 2018 and generated revenue of €1.56 billion in 2024, €1.2 billion of which came from Digital Solutions and Cloud. IONOS Cloud includes data centres in Germany, France, England, Spain and the USA (some of which are operated by partners). The range of services includes essential infrastructure services for computing, storage and networking. In addition, there are monitoring services and PaaS offerings for Kubernetes, databases and data analytics, as well as the AI service AI Model Hub.

Open Telekom Cloud

Based on Huawei's OpenStack distribution, the Open Telekom Cloud has been on the market since 2016 and has two regions, each with three availability zones

availability zones in Germany and the Netherlands, as well as two additional data centres in Switzerland.

Due to its relatively long history, OTC offers a comprehensive portfolio of cloud services. Recently, the focus has been on the introduction of AI Foundation Services, which allow customers to use various LLM models, among other things. Another focus of OTC is the development of tailor-made industry solutions.

OVHcloud

OVHcloud is the cloud offering from French telecommunications and hosting provider OVH, which has been on the market for over 20 years. OVH has a total of 43 data centres in nine countries (in Europe, in addition to France, in Germany, Poland and the United Kingdom, as well as in Canada, the United States, Australia, Singapore and India) and generated a turnover of €993 million in 2024. The range of services is very extensive and includes not only classic cloud services but also bare metal and hosted private cloud.

plussserver

Since the end of 2020, plussserver has had its own public cloud offering with basic IaaS services, but also provides managed databases, Kubernetes and AI. The company operates four data centres in Germany (Cologne, Düsseldorf and two data centres in Hamburg). In addition to its own cloud offering, plussserver also supports its customers in setting up multi-cloud environments.

Scaleway

The French company Scaleway operates nine data centres in Paris, Amsterdam and Warsaw. Scaleway was founded in 1999 and originally started out in hosting. In addition to classic IaaS services, Scaleway offers managed databases, AI services, as well as managed Kubernetes and serverless. Scaleway also offers dedicated servers and bare metal servers, including RISC-V servers.

STACKIT

The STACKIT Cloud is part of the financially strong Schwarz Group, which includes



ix workshop "Internal IT as a cloud provider – setting up a cloud competence centre"

By setting up their own Cloud Competence Centre, companies establish a central team that systematically builds, bundles and manages expertise and skills in dealing with cloud technologies. The Cloud Centre of Excellence (CCoE) acts as a central point of contact within the company for all cloud-related issues. It develops and establishes best practices and assumes a strategic and controlling role in the introduction of a cloud governance framework.

The workshop shows how a competence centre can be structured and set up to successfully drive cloud transformation within a company. Speaker Sebastian Tappe, Cloud Consulting Manager at Rewion GmbH, will present key components and show how a CCoE can effectively support the planning, implementation and operation of cloud projects.

Registration and dates at heise.de/s/rLAA5

The development began in 2018, and STACKIT Cloud has been available on the market since 2022. It consists of a central region in Heilbronn and data centre locations in neighbouring Ellhofen and Ostermiechting in Austria. Further locations are in the planning stage, including Lübbenau in Brandenburg. In the relatively short time since its market entry, STACKIT has launched an impressive number of services, and Schwarz IT is also investing heavily in security and AI.

Conclusion

Despite the dominance of American providers, a number of providers have established themselves on the European market, even if their market shares are still relatively small. It remains to be seen whether the current geopolitical tensions and the desire for independence will fundamentally change this situation.

A major challenge for new providers is the high level of investment required to set up and operate new data centre capacities. European cloud providers generally have a good basic range of services, particularly in the area of infrastructure, but also in terms of support for managed databases and Kubernetes.

Before choosing a provider, companies should analyse what they expect from the provider and whether it can meet those expectations. It is also advisable to follow the development of providers, as the number of new features and services is constantly growing. If customers are willing to accept the additional effort of a multi-cloud

Don't shy away from strategy; missing features or capacities can also be compensated for by using additional cloud providers.

Public Cloud made in Europe is a step towards greater digital sovereignty. Ultimately, every IT manager must decide for themselves what this is worth to them. (odi@ix.de)

DR CONSTANTIN SÖLDNER

is one of the managing directors of Söldner Consult GmbH. His areas of expertise include cloud infrastructure, automation and DevOps, as well as Kubernetes.



DR GUIDO-ARNDT SÖLDNER

is the managing director of Söldner Consult GmbH and deals with the topics of cloud computing and enterprise programming.



PROF. DR. JENS-HENRIK SÖLDNER

is Professor of Business Informatics and IT Security at Ansbach University of Applied Sciences and Managing Director of Söldner Consult GmbH.

