EXOSCALE
member of | A1 Digital

# Cloud-Computing: How Businesses can find the right Cloud Provider

## Legal, Economic and Technical Selection Criteria for Cloud Implementation

# Cloud-Computing: How Businesses can find the right Cloud Provider

## Legal, Economic and Technical Selection Criteria for Cloud Implementation

**Cloud computing has at this point arrived in Germany as well. Even as late as 2016, 17% of participants of the annual Bitkom Research and KPMG "Cloud Monitor" study declared the cloud to be a non-issue for them, but in 2022, that number had shrunk to just 3%[1]. German businesses however remain skeptical when it comes to the subject of public cloud resources (see definition in the box on page 6). According to current figures released by digital association Bitkom, only 55% of survey respondents use this resource, with an additional 29% planning or debating its implementation[2].**

This reluctance is understandable, as a step towards a public cloud requires careful consideration and planning, particularly for medium-sized businesses. There are many aspects to address, such as issues relating to data protection and sovereignty, legal compliance, and security. Complex tenders, high entry barriers and opaque pricing structures frequently deter potential users. There is however no doubt that a digital transformation without the use of a public cloud lacks the necessary urgency. Analysts at development bank KfW regularly complain about the slow pace towards digitalization in medium-sized businesses[3]. A recent study by KfW Research shows that delays in digitalization have a particularly detrimental effect on businesses with ambitious competitive strategies[4].

This whitepaper is designed to support medium-sized businesses in the quick and successful transition to the public cloud, providing decision guidance for selecting the right cloud provider while taking legal, economic and technical aspects as well as specific requirements faced by medium-sized businesses into consideration.

[1] https://kpmg.com/de/de/home/themen/2022/06/cloud-monitor-2022.html

[2] https://www.bitkom.org/sites/main/files/2023-05/230516Bitkom-ChartsCloud-Reportfinal.pdf

[3] https://www.kfw.de/%c3%9cber-die-KfW/KfW-Research/Digitalisierung.html

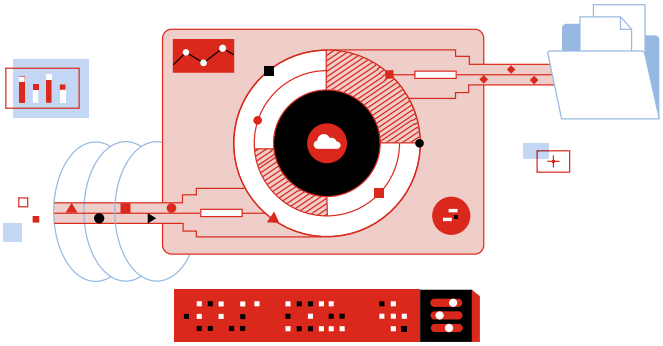
[4] https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-2023/Fokus-Nr.-432-Juli-2023-Digihemmnisse-Strategie.pdf

# 1 Legal Aspects of Cloud Selection: Data protection, IT Security, Compliance

## a) Data Protection

Since May of 2018, the General Data Protection Regulation (GDPR)[5] has been in effect in the European Union. It is designed to establish a high and consistent level of data protection in all member states. Businesses are only permitted to collect and utilize personal data with the express permission of the affected individuals. When collaborating with IT service providers or a cloud provider, the contracting party is responsible for complying with all regulations. Any violations can result in fines of up to 20 million euros or 4% of the respective violator's global annual turnover. Should any personal data falling under GDPR regulations be transferred to third party countries, a level of data protection akin to that of the European Union must be demonstrated. This is the case in Iceland, Liechtenstein and Norway for example, as these countries have adopted the General Data Protection Regulation act into their national legal framework. Japan and Switzerland are also considered to be countries providing adequate levels of data protection.

Legally problematic however, are transfers to US providers. The CLOUD Act (Clarifying Lawful Overseas Use of Data)[6], which came into effect in 2018, makes it mandatory for US companies to surrender client data to US authorities – even if the data isn't stored in the US. Affected individuals are not informed about their data being compromised, as US authorities can impose gag orders on the respective providers, effectively silencing them. For that reason, the European Court of Justice (ECJ) has repeatedly asserted that the US cannot provide an adequate level of data protection. In a July 2020 ruling (Schrems II)[7], it overturned the Privacy Shield agreement between the EU and the US, which was designed to enable a data protection-compliant exchange of data. This rendered legal transfers of personal data between the EU and the US virtually impossible without any additional guarantees.



Since July 2023, the successor to the Privacy Shield has been in effect, the EU-US Data Privacy Framework (EU-US DPF)[8]. It represents a so-called "adequacy deci-

[5] https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de

[6] https://www.justice.gov/criminal/cloud-act-resources

[7] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/EU_UN/Kernaussagen-Schrems-II.pdf?__blob=publicationFile&v=4

[8] https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752

sion", through which the European Commission declares the US to be able to provide a level of data protection similar to the EU. The EU-US DPF however is restricted to certified US organizations stating a clear commitment to compliance with the given data protection regulations. Further details can be found in the usage guide released by the Datenschutzkonferenz (data protection conference)[9], the official body of German data protection authorities.

It is questionable whether the EU-US DPF could withstand legal scrutiny by the ECJ, as the fundamental problems remain the same: data belonging to European businesses and citizens can still be accessed by US authorities. Organizations exchanging personal data with US providers therefore continue to take legal risks.

### b) IT Security

Cyber threats are considered the number 1 existential risk to the economic survival of businesses[10]. They also increasingly jeopardize the security and infrastructure supply of the general public – multiple healthcare institutions, local authorities and cities have already been victims of hacking. The latest cases include ransomware attacks on Frankfurt University Hospital in October 2023[11] and the German municipal IT service provider Suedwestfalen-IT in November 2023[12]. National and European legislators have subsequently been imposing gradually stricter requirements concerning but not limited to operators of so-called critical infrastructure (KRITIS). Notable examples are the German IT Security Act 2.0 (ITSIG), in effect in Germany since May 2021, and the EU Network and Information Security Directive NIS2[13], in force since January 2023 and mandated to be converted into national law by mid-October of 2024.

An informed selection of any cloud service has to take the supply chain security mandated by NIS2 into account. Affected businesses are required to not only

[9] https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

[10] https://www.allianz.com/de/presse/news/studien/230117_Allianz-Risk-Barometer-2023.html

[11] https://www.heise.de/news/Angriffsversuch-durch-Hacker-Uniklinikum-Frankfurt-offline-9328925.html

[12] https://www.heise.de/news/Nach-Ransomware-Angriff-Suedwestfalen-IT-und-Kommunen-lehnen-Loesegeldzahlung-ab-9386564.html

[13] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

comply with all regulations but to be able to verify that all of their suppliers and service providers equally maintain a level of security in line with legal requirements.

### c) Compliance

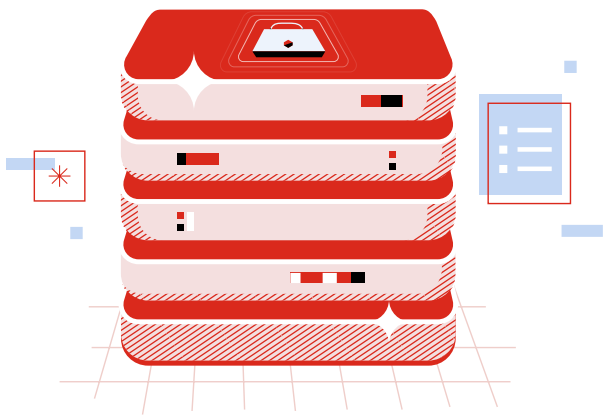
Any violations of current regulations may result in considerable economic consequences. The GDPR is not alone in mandating high financial penalties in cases of non-compliance; the NIS amendment has also significantly expanded the punitive scale. There, the maximum penalty is now 10 million euros. In cases of criminally relevant offenses such as embezzlement, violation of legal accounting obligations or environmental crimes, guilty parties can even face prison sentences. Crimes against competition, consumer or employment laws regularly lead to warnings, fines or compensatory damages.

Businesses are therefore required to establish measures ensuring management and staff conduct adheres to regulatory and legal requirements, collectively referred to as Compliance. Organizations should also ensure that all aspects of compliance are observed by their service providers and suppliers.

## Recommendations for Cloud Provider selection in light of Data Protection, Legislation and Compliance

1 Any collaboration with a US provider introduces significant legal risks despite the adoption of the EU-US Data Privacy Framework. Businesses should instead choose a provider with headquarters in Europe and operating data centers in the EU. This would ensure compliance with all GDPR requirements.

2 Going forward, companies affected by NIS2 are only permitted to collaborate with service providers demonstrating an adequately high level of security. They should therefore select a provider who meets these requirements and can verify this by submitting valid certificates, such as international security standards ISO/IEC 27001[14], ISO/IEC 27017 and ISO/IEC 27018.



[14] https://www.iso.org/standard/27001

3 Businesses need to have an overview of their compliance status at all times, to be able to identify potential risks quickly. A good cloud provider will produce all necessary information in a structured fashion in one spot.

## Types of Cloud Computing

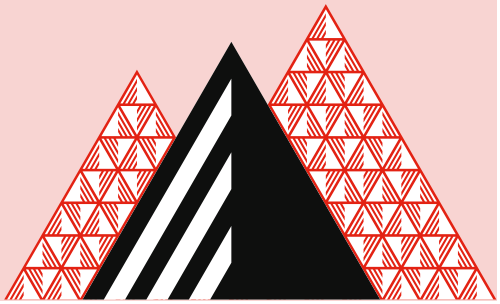
The NIST (National Institute of Standards and Technology) lists the following commonly defined types of cloud computing in existence:

**Private Cloud:** The cloud infrastructure is exclusively available to a specific company or department. Resources may be located at a company's own data center, a hosting provider or an internet service provider. Virtual private cloud services within a public cloud are also an option.

**Community Cloud:** Organizations sharing interests, structures or security requirements access a shared cloud infrastructure system, which can be operated by an internet service provider, a different specific service provider or one of the participating organizations themselves.

**Public Cloud:** The cloud infrastructure is publicly accessible via the internet. Security and privacy are guaranteed through data encryption during transfer and storage.

**Hybrid Cloud:** A mix of cloud types, typically combining public cloud resources with local IT infrastructure in order to absorb peaks in demand or to expand the range of services.



# 2 Economic Aspects of Cloud Selection: Costs, Data Sovereignty, Sustainability

## a) Costs

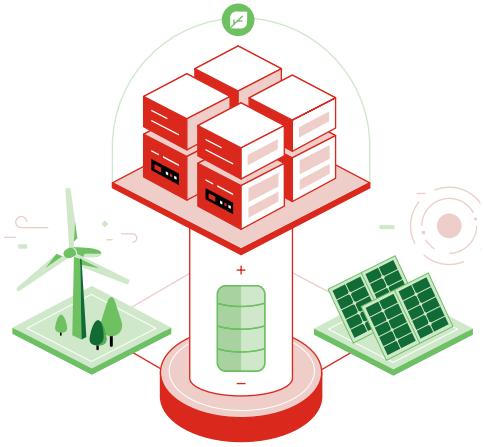
For many businesses, cloud computing is considered an affordable alternative to operating IT systems within their own data centers. As a matter of fact, in particular new resources and test environments can be built more quickly and inexpensively in a cloud environment than within a local data center. However, the price advantage can potentially have the reverse effect: the metered billing applied in the cloud means that high usage drives up costs. Unpleasant surprises may ensue if demand unexpectedly surges.

Businesses can also find themselves at a price disadvantage if demand is miscalculated from the start. Many cloud providers only offer long-term contracts or large-scale advance orders, but especially at the beginning, it is difficult to gauge cloud usage accurately. Overestimating demand will result in having to pay for unnecessary resources while underestimating and subsequently ordering at too small a scale may entail having to place additional orders at excessively high prices.

Hidden costs can also lead to unpleasant surprises. For example, many providers offer free data transfers in their cloud in one direction, but charge steep prices for return transfers. For organizations who want to switch providers or who regularly pull large amounts of data from the cloud, this can signify a considerable cost increase.

## b) Data Sovereignty

According to the definition coined by the Competence Center of Public IT[15], digital sovereignty means “the sum of all capabilities and possibilities available to individuals and institutions to perform their roles in the digital world in an independent, self-determined and secure manner.” For organizations, this primarily means that trade secrets are guarded, and internally generated data can be commercialized while being protected from unauthorized access. A significant part of data sovereignty is also the freedom to decide where and in what manner any business data is stored.



[15] https://www.oeffentliche-it.de/documents/10181/14412/Digitale%20Souver%C3%A4nit%C3%A4t

There is a risk of losing this sovereignty when transferring any data into the cloud. Unencrypted transfer and storage of information or even key management by the cloud provider can lead to a loss of data sovereignty. This makes the use of US cloud services problematic from a data sovereignty perspective, as there exists an obligation to surrender client data to authorities upon request for these service providers. From a European position, it can't be safely determined whether or not these authorizations will be used to lead to criminal prosecution or even abused for the purposes of industrial espionage.

### c) Sustainability

An increasingly important aspect of business operations is being energy- and resource-efficient. Alongside budgetary issues and climate change, more and more businesses are now legally required to act sustainably. In January 2023, the Corporate Sustainability Reporting Directive (CSRD)[16] came into effect, making it mandatory for organizations to report on their sustainability initiatives. For now, this directive only applies to businesses with more than 500 employees, but this will be significantly expanded by 2028.

Affected businesses are required to account for their non-financial activities in an annual report, which must comply with European Sustainability Reporting Standards (ESRS). Not only must they document any relevant internal activity, but they are also required to demonstrate that their suppliers and IT service providers equally adhere to given sustainability and social standards.

## Recommendations for Cloud Provider Selection from a Cost, Data Sovereignty and Sustainability Perspective

1 When choosing a provider, businesses should keep an eye out for fair, metered billing without any hidden costs, and stay away from long-term binding contracts and complicated pricing structures.

2 In terms of data sovereignty, businesses should choose a provider with headquarters and data center operations in Europe.

3 The provider should be able to verify their sustainable and energy-efficient business practices, and any data should be readily available for client companies to incorporate into their sustainability reporting.

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464

# 3 Technical Aspects of Cloud Selection: Scope of Service, Complexity, Support

## a) Scope of Service

Alongside the traditional classification into IaaS, PaaS and SaaS (see text box on page 10), the range of cloud services available continues to expand and diversify. For medium-sized client businesses, an optimal balance between adequate scope of service and clear, concise structure tends to be a decisive factor. If essential services are missing, business development will be hampered. If on the other hand the range of options offered is too vast and overwhelming, too many resources will be wasted trying to compare and choose the appropriate service.

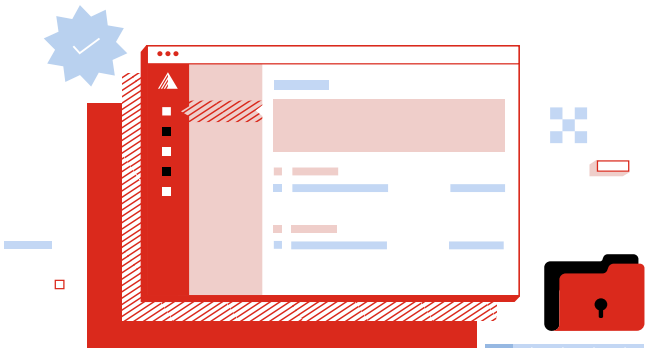
## b) Complexity

There is a distinct skilled labor shortage in the IT sector. According to the Cologne Institute for Economic Research, there were 34.000 vacancies for IT professionals in 2022, which could not be filled. A recent European SME Survey indicates that in medium-sized businesses, the shortage of IT professionals is particularly pronounced[17].

However, many cloud services require a high level of expert knowledge and intense training. Large companies very often employ several cloud architects whose only task it is to design cloud environments, something that's generally not feasible for medium-sized businesses. Adequately competent professionals are expensive and difficult to find, rendering the financial and resource expenditure too high a price to access cloud computing. It is therefore not surprising that a lack of qualified personnel is listed as the most common obstacle to cloud implementation, according to the Bitkom Cloud Report 2023[18].

## c) Support

Cloud computing is marked by a high availability and a certain robust character when it comes to errors. Even so, occasional cloud outages still occur, such as the one experienced in 2021 with cloud provider Amazon Web Services[19]



[17] https://op.europa.eu/en/publication-detail/-/publication/12f499c0-461d-11ee-92e3-01aa75ed71a1/language-en

[18] https://www.bitkom.org/sites/main/files/2023-05/230516Bitkom-ChartsCloud-Reportfinal.pdf

[19] https://www.heise.de/hintergrund/Die-technischen-Hintergruende-von-Amazons-AWS-Ausfall-6293942.html

and the one suffered by Microsoft Cloud Azure in early 2023[20]. When this type of outage happens, small and medium-sized clients in particular often receive little or no information, and are left to their own devices cleaning up the resulting damage such as a loss of customers or revenue.

Furthermore, the general lack of adequate support is not felt merely during cloud outages. When basic questions about product details or settings are left unanswered, and IT staff find themselves chatting to a bot or endlessly holding the line on a call, it not only negatively affects the user experience but potentially also system or data security, as cloud resource configuration errors count among the biggest risks in cloud computing[21]. Fast and individual support is therefore a critical factor in cloud selection.

## THE THREE LEVELS OF CLOUD SERVICES

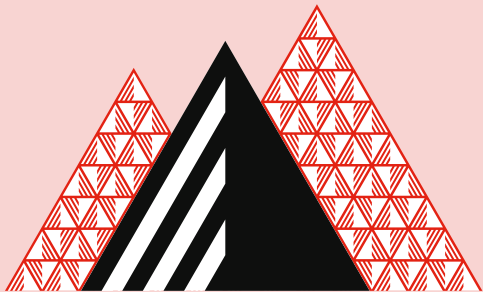
Cloud-Services can generally be classified into three service models:

**Infrastructure as a Service (IaaS):** The provider offers server, storage and network components. Businesses can use these to install and run their own operating systems and applications. The components are usually presented virtually, but there are also so-called bare-metal services, which allow for direct access to hardware resources.

**Platform as a Service (PaaS):** The cloud provider offers a platform featuring an operating system, middleware and development tools. Businesses can use this as a basis to develop and operate their own applications.

**Software as a Service (SaaS):** This service model offers applications as service. Access is typically browser-based and therefore device-independent.

Source: National Institute of Standards and Technology (NIST)



[20] https://www.heise.de/meinung/Kommentar-zum-Cloud-Ausfall-bei-MS-Ist-der-Patient-schon-tot-oder-nur-laediert-7484066.html

[21] https://cloudsecurityalliance.org/blog/2022/08/22/top-threat-3-to-cloud-computing-misconfiguration-and-inadequate-change-control/

### Recommendations for Cloud Provider Selection based on Scope of Service, Complexity and Support

1 The best choice of cloud provider should offer all the services a business needs. A clear, concise structure and a focus on the essentials present major advantages, while an excessively varied and detailed offer can quickly seem overwhelming.

2 For the initial steps into cloud computing, simple, coherent and user-friendly services are recommended. Ideally, the cloud provider will support the onboarding process with information and training material.

3 Only the emergence of issues or questions really shows whether a provider is actually client-friendly. Global corporations often see medium-sized business clients as just a number, and relegate them to the chatbot and similarly automated resource corner. Businesses are advised to watch out for support on equal terms and favor providers who offer personal points of contact from the very start.

## Conclusion: a Successful Journey to the Cloud requires the Right Partner

Cloud computing is an essential digitalization strategy component, also for medium-sized businesses. However, achieving this at the necessary speed is hampered by legal requirements, tight budgets, and a shortage of IT professionals. Businesses therefore need a cloud partner like Exoscale, who meets all above-mentioned criteria and supports businesses on their journey towards cloud use. Headquartered in Switzerland and operating all its data centers in Europe, this provider fully complies with GDPR requirements and covers all essential security criteria. With the click of a button, businesses are easily able to verify the legal compliance status of their cloud usage.

Even from an economic perspective, Exoscale is persuasive: usage cost is metered, so invoicing is exact and fair, without any contractual commitments or complicated tariff structures. Cloud data transfer is free up to a terabyte of volume per event, per month. All data is stored in European data centers, and businesses retain full resource sovereignty. Exoscale is also committed to sustainable and environmentally friendly business practices, and accounts for all business activities via their parent company A1's annual ESG (environmental, social, governance) report. The provider aims to utilize 100% renewable energy by 2025, and all its sustainability certificates can already be viewed via the previously mentioned Compliance Center.

Ultimately, Exoscale presents many technical advantages as well. This provider's portfolio includes all services relevant to medium-sized businesses without being overloaded with hundreds or thousands of different extras. Getting started is easy, and in case of problems or questions, business clients have access to first level contact with developers right from the start. Additionally, the Exoscale Academy provides training courses and offers any necessary certifications for free.

**Try Exoscale Now – Commitment-free, and at Zero Cost >**

## Check list

### Questions to Ask any Service Provider

- ✓ Are data centers located in the European Union? Does the data storage comply with GDPR regulations? Can foreign authorities force access to any data?
- ✓ Can the provider verify that it is compliant with all legal requirements? Do they offer security certificates, and if yes, what are they?
- ✓ How can business clients document that their cloud service use complies with all regulations?
- ✓ What does the cost structure look like? Is it simple and easy to understand or are there any complicated tariffs and hidden costs? Is getting started a quick process or does it require high up-front investment and a long contractual commitment?
- ✓ Does the provider adhere to sustainable, environmentally friendly business practices? How are any sustainability initiatives documented?
- ✓ Does the cloud platform offer all essential services without being too complicated or presenting too many options? How easy is getting started?
- ✓ What type of support does the provider offer? In case of a problem, is a real person or merely a chatbot the first point of contact?
- ✓ How does the provider support clients during the onboarding process? What kind of training courses or certifications are offered?


# EXOSCALE

Exoscale, founded in 2011, is a member of A1 Digital and belongs to the Telekom Austria Group. The cloud provider with its headquarters in Switzerland supports businesses and engineers in operating their workloads and applications securely in the cloud. Its user-friendly, reliable and high-performing cloud platform makes Exoscale the ideal partner for cloud-native applications. Our focus on security and data protection also ensures continuously smooth and GDPR-compliant cloud use.

**Contact >**

EXOSCALE
member of | A1 Digital