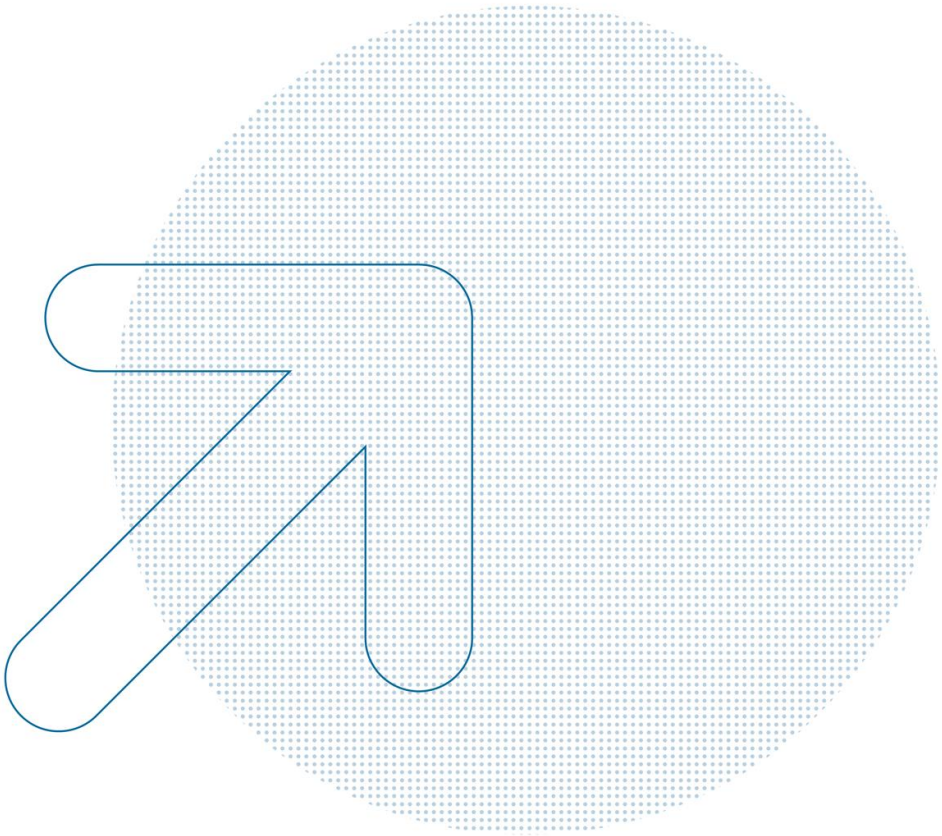
WIK-Consult • Report

Study for the Bundesnetzagentur



Study on the classification of data processing services when switching provider pursuant to the Data Act

Exit report

Translation provided by Bundesnetzagentur

Bad Honnef, 25 June 2026

WIK CONSULT

Publisher's details

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
Email: info@wik-consult.com
www.wik-consult.com

Persons with authority to represent and sign

Board of Directors	Dr Cara Schwarz-Schilling (Chair of the Management Board)
	Alex Kalevi Dieke (Chief Financial Officer)
Authorised representatives	Professor Bernd Sörries
	Dr Christian Wernick
	Dr Lukas Wiewiorra
Chair of the Supervisory Board	Dr Thomas Solbach
Registered at	Amtsgericht Siegburg, HRB 7043
Tax no.	222/5751/0926
VAT-ID	DE 329 763 261

Authors:

Peter Kroon (Engineer, WIK-Consult), Professor Anne Paschke (TU Braunschweig), Mark Reeve (Decision), Christian Märkel (WIK-Consult), Malte Roloff (WIK-Consult), Desislava Sabeva (WIK-Consult), Martin Lundborg (WIK-Consult)

Translation disclaimer

This document is an English translation provided by the Bundesnetzagentur and is intended for informational purposes only. While every effort has been made to ensure the accuracy of the translation, in the event of any discrepancies or differences in interpretation, the original German-language version shall prevail.

Contents

List of figures III

List of tables III

EXECUTIVE SUMMARY [EN] V

1 Introduction 1

2 Development of an assessment framework for data processing services 3

2.1 Systematic interpretation of the concept “data processing service” 3

2.1.1 Explanation of the components of a data processing service 3

2.1.2 Supplementary (overall) assessment 16

2.1.3 Services not included 19

2.2 Development of the assessment framework for identifying data processing services 23

2.3 Limits of the assessment framework and consequences resulting from them 27

2.3.1 Structural scope for interpretation of the legal definition 27

2.3.2 Grey zones and borderline cases 27

2.3.3 Addressing of scopes for interpretation 28

3 Establishment of a classification model for “same service types” 29

3.1 Structured interpretation of the concept “same service type” 29

3.1.1 Main objective 30

3.1.2 Service model 31

3.1.3 Main functionalities 32

3.1.4 Overall assessment 33

3.2 Derivation and operationalisation of suitable classification criteria 34

3.2.1 Literature overview 34

3.2.2 Proposed main objectives of data processing services 47

3.2.3 Proposed main functionalities of data processing services 47

3.2.4 Identification of the service models of data processing services 49

3.2.5 Proposed classification 50

3.3 Analysis of modular / partial switch of services 55

3.3.1 Definition of a “modular switch” 55

3.3.2 Different scenarios for unbundling 56

3.3.3 Five-step approach to the analysis of modular switching 57

3.3.4 Unbundling of individual cloud services offered via different provisioning models 59
3.3.5 Application of the methodology to real use cases and grey zones 61
3.3.6 Results of the interviews 63
3.4 Testing of the developed classification model 69
4 Market overview of data processing services 73
4.1 Identification of the key providers in the cloud market of the EU 73
4.1.1 Glance at the overall market 73
4.1.2 The IaaS market 75
4.1.3 The PaaS market 77
4.1.4 The SaaS market 79
4.1.5 Condensed overview of the identified cloud providers in the EU 81
4.2 Identification and classification of the data processing services of the identified providers 82
4.3 Classification of the identified data processing services using the classification model 84
5 Analysis of practical application challenges 92
5.1 Distinction of non-permissible “specific support activities” from services that providers may continue to charge for 92
5.2 Interpretation of the exemption provisions set out in Article 31 of the Data Act 95
6 Conclusion 106

List of figures

Figure 2-1: Data processing service assessment framework 24

Figure 3-1: Determination of the “same service type” 30

Figure 3-2: Illustration of an application run in an IaaS environment 44

Figure 3-3: Illustration of an application run in an PaaS environment 44

Figure 3-4: Illustration of an application run in an SaaS environment 45

Figure 3-5: Overview of the testing of the model 69

Figure 4-1: Market shares on the overall public cloud market 74

Figure 4-2: Breakdown of the market to the service models IaaS, PaaS and SaaS 74

Figure 4-3: Participants on the IaaS market 75

Figure 4-4: Participants on the PaaS market 77

Figure 4-5: Participants on the SaaS market 79

Figure 4-6: Aggregated overview of the identified providers 82

Figure 4-7: Classification of the identified data processing services using the classification model 85

Figure 5-1: Delimitation and categories of actions 95

List of tables

Table 3-1: Initial step towards taxonomy 48

Table 3-2: Proposed classification model 52

Table 3-3: Illustration of the interpretation of the classification model based on an excerpt from the model 54

Table 4-1: Primary sources concerning the services of cloud providers 83

Table 4-2: Assessment of the services of cloud providers 87

Table 4-3: Breakdown of confidence levels across all services 88

Table 4-4: Aggregated allocation of cloud providers investigated in the classification model 89

Table 5-1: Delimitation criteria for support actions 93

Table 6-1: Illustration of the structure of the classification model in section 3 106

EXECUTIVE SUMMARY [EN]

This study systematically analyses the switching provisions applicable to data processing services under Chapter VI of the Data Act. By integrating legal, technical and economic perspectives, it aims to support the legally sound and practically workable implementation of the requirements governing switching between cloud service providers. Particular emphasis is placed on developing a consistent assessment framework for determining what constitutes a service, defining the concept of the "same service type" in the dynamic cloud market, establishing a classification system for identifying services of the same type, and resolving structural problems arising in the application of the provisions.

A key element of the analysis is therefore the delineation of services, since the switching provisions of Chapter VI of the Data Act apply only where the service being switched from and the service being switched to are considered to be of the "same service type". Accordingly, the delineation and classification of services are of considerable importance.

Assessment framework for data processing services

As a first step, it must be determined whether the service in question constitutes a data processing service within the meaning of the Data Act. For this purpose, the present study develops a systematic assessment framework based on Article 2(8) of the Data Act. If all stages of the assessment are satisfied, the service may be considered a data processing service within the meaning of the Data Act. More detailed information on the assessment framework is provided in Chapter 2 of the study

Classification model for determining the "same service type"

If the service in question constitutes a data processing service within the meaning of the Data Act, the next step is to assess whether the source service and the destination service are of the same service type. Services may be considered to be of the same service type if they share the same service model, the same main objectives and the same main functionalities.

To determine whether services are of the same service type, this study develops a comprehensive classification model covering all relevant levels, namely the service model, main objectives and main functionalities. This is likely to constitute the first comprehensive attempt in the academic literature to classify services in accordance with the definition of the "same service type" under the Data Act.

The analysis showed that the three levels of service model, main objective and main functionality are not sufficient to determine or delineate the same service type unambiguously. Accordingly, the relevant technical interfaces were examined, taking into account the subcategories of service types, in order to enable the practical assignment of a service to a particular service type. The complete classification model is presented

in Chapter 3 of the study. Testing of the model demonstrated that it is suitable for this purpose, although certain borderline cases remain.

Analysis of modular switching

The situation becomes even more complex where a modular switch is envisaged, that is, where the customer wishes to switch only a specific individual service while retaining the remaining adjacent services with the original provider. This issue was also examined in the present study. For this purpose, expert interviews were conducted with both cloud providers and cloud customers.

The findings indicate that, with regard to the technical feasibility of such modular switching, a distinction must be drawn between the different service models. While modular switching at the Infrastructure-as-a-Service (IaaS) level generally poses no major technical difficulties, the situation differs at the Platform-as-a-Service (PaaS) level and, in particular, at the Software-as-a-Service (SaaS) level. Especially in the business environment, these services are commonly tailored to the specific requirements of individual undertakings. As a result, they are less standardised and cannot readily be migrated to another provider.

The interviews with cloud customers also showed that modular switching is relatively unattractive from the customer's perspective. Owing to providers' pricing models, such a switch would often result in higher prices for the services retained with the original provider. Against this background, modular switching is therefore unlikely to be of substantial practical relevance for as long as such pricing models remain in place. A detailed analysis of modular switching is also provided in Chapter 3.

Classification of services offered by major providers

Following the development of the classification model, a total of 19 major providers operating in the IaaS, PaaS and SaaS markets were identified on the basis of current market data. An AI-assisted analysis was then conducted to compile as comprehensive an inventory as possible of all data processing services offered by these providers. The services were subsequently assigned to the previously developed classification model.

Of the 2,964 services examined, 2,536 could be assigned to the taxonomy with a high degree of confidence, which is equivalent to 87%. This result confirms the practical applicability of the classification model. The analysis of the providers and the classification of their services are presented in Chapter 4.

Application challenges

Finally, the study analysed two challenges arising in the application of Chapter VI of the Data Act.

First, it examined the issue of switching charges. In particular, the study assessed which forms of assistance provided in connection with switching may no longer be charged separately from 12 January 2027 onwards. Charges will no longer be permissible for activities that form part of the provider's statutory obligation to enable switching, including, in particular, technical assistance, data extraction, testing, switching-related documentation, necessary tools and security measures. By contrast, providers may continue to charge for standard services and for additional migration services expressly commissioned by the customer, such as project management, in-depth consultancy, code adaptations, training or professional transition services.

Second, the study examined the interpretation of the exemption provisions set out in Article 31 of the Data Act. Under these provisions, certain customer-specific data processing services, as well as services provided solely for testing and evaluation purposes, are wholly or partially exempt from the switching obligations laid down in Chapter VI. To make the legal effects of Article 31 more tangible, however, it is necessary to interpret the indeterminate legal concepts used in that provision. Accordingly, the study interprets the terms central to Article 31 of the Data Act, namely "majority of main features", "broad commercial scale", "custom-built", and "testing and evaluation purposes", thereby contributing to greater legal certainty. The results of the discussion of these application challenges can be found in Chapter 5 of the study.

Conclusion

The present study has succeeded in developing a classification model for determining the "same service type" within the meaning of the Data Act. The model makes it possible to assign almost 90% of the services offered by major providers to the relevant categories under the Data Act with a high degree of confidence. It may therefore assist supervisory authorities, providers, customers and the academic community in the interpretation and application of the relevant provisions.

At the same time, the analysis has demonstrated the considerable practical complexity of the switching provisions laid down in Chapter VI of the Data Act. Moreover, the cloud market is highly dynamic, both technologically and economically, and any classification system must be continuously adapted to developments in the market. Accordingly, the cloud providers and cloud customers interviewed currently take a cautious view of the practical impact of the Data Act's switching provisions.

The actual effects of the regulation on the market should therefore continue to be closely monitored. Should the regulation fail to produce its intended effects, an amendment of Chapter VI of the Data Act should be considered. Possible reforms could include simplifying the definition of the "same service type" and placing greater emphasis on IaaS and, where appropriate, PaaS services, since both the delineation of services is more practicable and the need for market-structural intervention is greatest in these segments.

1 Introduction

The purpose of this study, conducted on behalf of the Bundesnetzagentur, is to systematically identify, illustrate and analyse the core principles and practical issues concerning the switching provisions for data processing services in the Data Act (Chapter VI).

The focus is placed on the delineation of services, the development of suitable classification and categorisation systems and the assessment of practical application challenges to support legally sound and practicable implementation of the requirements of the Data Act.

To this end, this study particularly addresses the following three research questions that integrate legal, technical and economic perspectives:

- How can the broad concept of a data processing service be translated into a consistent and verifiable assessment framework?
- How can the “same service type” be defined and operationalised to ensure its practical applicability in a dynamic cloud market?
- Which application problems arise from the norm structure of Chapter VI and how should they be appropriately addressed?

Section 2 lays the foundation by drawing up a systematic and academically substantiated interpretation of “data processing service” as a core concept of the Data Act and deriving from this an assessment framework for the existence of a data processing service.

As the centrepiece of the study, section 3 establishes a functional classification model for precisely determining the “same service type” within the meaning of the Data Act. To this end, the service models, primary objectives and main functions of the data processing services are systematically identified as comprehensively as possible to establish when the same service type exists. The analysis pays particular attention here to the modular switching of data processing services. The findings from 10 expert interviews conducted with cloud providers and cloud customers are incorporated into this section to validate the results.

Section 4 follows on directly from the preceding section by compiling a market overview of the data processing services of relevant providers on the basis of the established classification model. The relevant providers are identified in a first step before in a second step the data processing services they offer are classified in the model using modern AI-assisted analysis methods.

Application challenges arising from Chapter VI of the Data Act are the topic of section 5. On the one hand, the issue of switching costs is addressed, specifically the distinction of non-permissible “specific support activities” from services that providers may continue to

charge for (section 5.1). Secondly, the interpretation of the exemption provisions set out in Article 31 of the Data Act is analysed (section 5.2). The study closes with a conclusion (section 6).

2 Development of an assessment framework for data processing services

2.1 Systematic interpretation of the concept “data processing service”

2.1.1 Explanation of the components of a data processing service

A “data processing service” (German: Datenverarbeitungsdienst; French: service de traitement de données; Spanish: servicio de tratamiento de datos) **within the meaning of Article 2(8) of the Data Act is**

- **a digital service** (German: eine digitale Dienstleistung; French: un service numérique; Spanish: servicio digital)

The Data Act does not contain any autonomous legal definition of the term “digital service”. However, the concept can be systematically determined on the basis of legal definitions of “digital services” and “ICT services” under EU law that can be drawn on in the context of data-related regulation.

An “ICT service” within the meaning of Article 2(13) of Regulation (EU) 2019/881 (Cybersecurity Act) is defined as a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems. In addition, Article 1(1) b) of Directive (EU) 2015/1535 defines the term “digital service” as any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (see also Article 6(23) NIS 2 Directive).

No actual liability to pay costs is required for this, see the provision in Article 23 c) of the Data Act. According to the general rule/exception principle, the consideration is not constitutive, which is also confirmed by recital 78 sentence 2.

This service does not necessarily have to be provided entirely by the provider of the service itself. Instead, certain tasks can be outsourced and performed by third parties, see recital 89 sentence 1.

Accordingly, a digital service exists when a service is essentially provided by electronic means, is typically available remotely via a network, is provided at the individual request of the user and is focused in terms of content on transmitting, storing, retrieving or processing information. With this in mind, cloud services regularly comprise digital services or ICT services because they make computing resources and data-related functionalities available via network and information systems. In addition, edge services also fall under this definition, see recital 78 sentence 1.

Examples: cloud storage (storing/retrieving), virtual machines or containers (processing), database services (retrieving/processing), SaaS applications (processing and storing), managed network services (transmission).

Negative delineation: purely physical or local services not provided at a distance and without electronic means (eg a hardware delivery), mere consulting or support services not relating predominantly to electronic information processing, and internal own work without service provision to a recipient are not included.

- **to a customer** (German: die einem Kunden; French: à un client; Spanish: a un cliente)

The “customer” is defined legally in Article 2(30) as “a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services”.

The customer is therefore exclusively the contracting party of the provider. Users of the service, employees of the contracting partner and third parties are not customers. This is a contractual relationship under civil law from which mutual rights and obligations are derived. It does not therefore include de facto use without a contract. As this definition is based exclusively on the contracting partner status, whether the contracting partner is a subsidiary within a group or an external company has no significance for the customer status. There are no requirements concerning the type of contract (eg rental contract, lease contract, contract sui generis) or the form of contract conclusion. It is furthermore of no significance whether just one or multiple data processing services are used.

Examples: a company has a cloud computing agreement, a bank makes contractual use of managed database services, a public institution has a contract for use of a data analytics platform, a private individual holds a contract governing a storage and backup service, a freelancer rents additional computing resources, a sole proprietor leases SaaS for data processing. (all cases involve a direct contract with the provider of the corresponding service)

Negative delineation: the mere user of a service without a contract with the provider (eg end customer of a reseller with no contract with the provider; employee of a company that makes a corresponding service available to its staff via company accounts; website visitor with no contractual relationship with the data processing provider; user without an account with guest access).

- **that is provided** (German: bereitgestellt wird; French: qui est fourni; Spanish: que se presta)

Provision refers to the technical provision of computing resources or functionalities by the service provider so that they can be used by the customer. The term “provide” thus covers the entirety of technical processes by which a service or individual resources are made

operational and assigned to the customer. These particularly include the provisioning (creation) of the resource, its configuration (eg allocation of capacities, network settings, permissions) and activation and launch to make direct access possible via a portal or API. The decisive factor here is the technical possibility of provision. Actual use by the customer is not necessary.

This provision typically takes place in a standardised, automated and needs-based manner to facilitate short-term use without the customer having to acquire its own hardware or the provider having to perform any manual action in individual cases.

***Examples*:** creation and launch of a virtual machine (VM) with a specific CPU and RAM configuration, creation of a storage area (block or object storage) for files and backups, provisioning of a database instance (including access data and network sharing), provision of a Kubernetes (K8s) cluster or individual container workloads or activation of a load balancer via the cloud portal.

***Negative delineation*:** purely organisational or legal services (eg consignment of contractual documents, consulting, support communication) and merely granting user rights without technical activation do not count as "provision" in the typical cloud-related meaning. The mere provision of a processing result (eg reports) is likewise not counted if the customer is not granted any proprietary access to the underlying resources.

- **ubiquitous** (German: und einen ortsunabhängigen; French: en tout lieu; Spanish: ubicuo)

The term "comprehensive" was used here in the original wording. However, this was changed to "ubiquitous" by way of a linguistic correction on 9 September 2025.[1] Recital 80 sentence 1 already used the term "ubiquitous" in this connection in the original wording. The term "ubiquitous" is used in recital 80 sentence 4 to describe the computing capabilities provided over the network and accessed through mechanisms promoting the use of heterogeneous thin or thick client platforms (from web browsers to mobile devices and workstations). The term "ubiquitous" is thus typically used in the context of digital services to describe a **broad geographic availability** or availability across different parts of an area (eg EU-wide, nationwide or international). It accordingly boils down to the network not just being accessible via a physical location.

"Ubiquitous" therefore means that a service is not just offered and available here and there or locally but on a larger geographic scope. In the cloud context this can refer both to the **availability of the service** (access via the internet for customers in many regions) and the **technical infrastructure** (eg multiple data centre locations, regions or availability zones). "Ubiquitous" therefore does not necessarily also imply actual availability at all

1 Official Journal L of 9 September 2025.

supply locations. The decisive factor instead is that the service is reliably accessible and usable in the target area.

***Examples*:** cloud service with EU-wide provision across multiple regions, global SaaS service with access from many countries, infrastructure distributed across multiple data centres for regional performance optimisation.

***Negative delineation*:** services only offered in a strictly confined area (eg only one local data centre without external availability), regional special solutions with access restrictions and systems that are in effect only available to a small group of users or at a small number of locations (eg pure intranet/on-site solutions) are not ubiquitous.

- **and on-demand network access** (German: und auf Abruf verfügbaren Netzzugang; French: un accès par réseau à la demande; Spanish: un acceso de red y bajo demanda)

“On-demand network access” means that customers can access and use the computing resources provided **remotely** via a network, typically the internet or private network connections, **at all times according to their needs**.

“On-demand availability” exists if access is not only possible at specific times and following individual activation, but can fundamentally take place **directly** and **as required**. “Network access” refers to technical access via standardised communication channels and protocols such as web interfaces, APIs or remote connections. Remote access typically comprises both use of the resources (including the execution of workloads) and their administration (provisioning, configuration, monitoring).

The term distinguishes typical cloud solutions from solutions that provide IT services but are not made available in a network-based self-service model that is retrievable at all times, but instead shaped largely by manual processes or local access options.

***Examples*:** access to cloud resources via web consoles and APIs, remote administration of a VM, access to object storage via HTTPS, database access via private network connections (VPN/private link), retrieval of serverless functions via HTTP requests.

***Negative delineation*:** there is no “on-demand network access” if access is only possible locally (without remote access), via manual activation or exclusively via individual operator actions. Purely physical data transfers using data carriers or services where customers do not receive any autonomous remote access to resources and administration but are merely delivered the results of processing also do not count.

- **to a shared pool of** (German: zu einem gemeinsam genutzten Pool; French: à un ensemble partagé; Spanish: a un conjunto compartido)

A “shared pool of computing resources” is a core component of typical cloud services. What it means is that the computing resources supplied by the service provider are not reserved **exclusively for one single customer** but are available to multiple customers as **bundled total capacity**. Recital 80 sentence 6 uses the term “shared pool” to describe “those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment”.

A “shared pool” thus refers to a technical resource base (including servers, storage, network components, virtualisation layer) that can be used to assign capacities to individual customers **according to their needs**. The distinctive feature is that while joint use is made of the resources, it is regularly organised via technical mechanisms (eg virtualisation, client separation, access controls) in such a way that customer environments remain separated from each other. The pool therefore particularly facilitates scalability and elasticity as resources can be dynamically distributed and returned to the pool when no longer needed.

The term encompasses both physically shared infrastructure (shared hardware) and logically shared resources, such as in the form of virtualised or containerised environments. The decisive factor is not whether a customer receives dedicated virtual resources but whether the underlying capacity comes from a jointly managed overall resource base.[2] Typical cloud pooling is frequently based on virtualisation and orchestration technologies that abstract physical infrastructure and split it into isolated utilisation units without removing shared use of the underlying capacity. Virtual machines or containers therefore merely comprise a logical allocation, while the physical computing, storage and network infrastructure remains part of a shared resource pool. Furthermore, a link to mere virtual exclusivity would misconstrue the way modern cloud architectures work and contradict the concept of pooling as cloud providers frequently also scale, relocate and reallocate seemingly “dedicated” environments dynamically from central clusters. The key factors are therefore central resource management and flexible redistribution from a shared capacity pool, not the isolated picture from the customer perspective.

***Examples*:** multi-tenant cloud infrastructure, multi-client provider, virtualisation cluster, Kubernetes cluster with multiple namespaces/tenants, shared object storage with logical separation, shared database platform with separate instances/schemas.

***Negative delineation*:** there is no shared pool if resources are assigned permanently and exclusively to one customer and not allocated dynamically from a shared capacity pool (eg fully dedicated hardware without pooling). Mere single-server solutions (“single

2 See also Bomhard MMR 2024, 109 (110).

tenant/single server") with scaling carried out only by way of individual procurement or manual expansion also do not count.

- **configurable,** (German: konfigurierbarer; French: configurables; Spanish: configurables)

In the context of digital data processing services, "configurable" describes the technical property of a service enabling users to **configure and adjust** specific parameters, properties and operating modes without the need for any individual software development or manual intervention on the part of the service provider.

"Configurable" accordingly means that the service is **adaptable** within a predetermined framework, such as in terms of performance parameters, access rights, security options, scaling rules or network settings. Recital 80 sentence 1 mentions the term "on-demand" in this connection. Configuration typically takes place via user interfaces, APIs or Infrastructure as Code (IaC). Configurability should be distinguished from genuine custom developments. A configuration only uses predefined options, while a development creates new functionalities. Configurability is frequently a prerequisite for customers being able to use resources according to their needs and changes being possible without significant administrative outlay. However, the possibility of configuring one or a small number of predefined options suffices in the present case to fulfil this requirement. As the legislator does not envisage any minimum requirements in this connection, it is not necessary to set any particularly high standards here.

It does not matter whether the customer is able to initiate the configuration by themselves. It suffices for the service to be adjustable by the provider.

***Examples*:** selection of CPU/RAM sizes, configuration of auto-scaling rules, configuration of firewall rules/security groups, configuration of IAM roles and authorisations, backup intervals and retention periods, selection of region/availability zone, database parameters, logging/monitoring configuration.

***Negative delineation*:** services are not "configurable" if they are only provided as a fixed standard product without configuration options and adjustments are only possible by way of individual programming, change requests or manual interventions by the provider. Purely organisational configurations (eg internal process instructions) also do not count as the service cannot be configured technically.

- **scalable and** (German: skalierbarer und; French: modulables et; Spanish: modulables y)

Scalability describes the ability of a service to **adjust** the computing resources provided **according to need**. Recital 80 sentence 5 defines the term as referring to computing resources that are flexibly allocated by the provider of data processing services, irrespective of the geographical location of the resources, to handle fluctuations in

demand. Proof of this ability takes the form of a contractual-functional interpretation of the contractually guaranteed service to the customer.[3]

Scalability is therefore a generic term for a business model that possesses the ability to alter computing resources such as CPU, RAM, storage or network performance **depending on the actual need**. Scaling can take place both vertically (more performance per instance, “scale-up/scale-down”) and horizontally (more instances simultaneously, “scale-out/scale-in”). Technical implementation can vary, for example through the physical addition of a server or augmented reality of existing systems. As the term “scalability” does not contain any time component, these changes can also be spread over a prolonged or appropriate period.

Scalability frequently presupposes that the resources are held in reserve and the adjustment is also technically possible. Some literature sources therefore consider this feature to offer an opportunity for services to “remove themselves by definition” from the scope of application of the norm.[4] However, as the legislator does not envisage any minimum requirements in this connection, it is not necessary to set any particularly high standards for scalability. In particular, a limited preselection according to different GB and TB volumes or predefined resource packages does not mean that the scalability requirement is not met as otherwise providers would easily be able to remove themselves from the scope of application of this provision by improving the structuring of their offerings.

It also does not matter whether the customer is able to initiate scaling with regard to the proprietary service by themselves. It suffices to fulfil this requirement for the service to be adjustable by the provider.

***Examples*:** increase in CPU/RAM of a VM, addition of further application servers behind a load balancer, expansion of storage, scale-up of a database instance (more compute), addition of Kubernetes nodes.

***Negative delineation*:** services with capacities that can only be expanded by means of a subsequent long-term procurement, manual hardware installations or individual project work are not scalable. Systems that do not permit any real increase in underlying computing resources (mere “licence scaling” without any technical capacity expansion) also do not count.

- **elastic** (German: elastischer; French: variables; Spanish: elásticos)

According to recital 80 sentence 6, the term “elastic” is used to describe those computing resources that are provisioned and released according to demand to rapidly increase or decrease resources available depending on workload. In contrast to the concept of

3 For a detailed discussion of the difference between a purely technical and a contractual-functional interpretation, see Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
4 Freiberg/Niebuhr, BB 2025, 1067 (1069); Siglmüller, MMR Beil. 2024, 112 (114).

scalability, the concept of elasticity therefore comprises a temporal component that is frequently implemented through the automation of scalability in accordance with a contractual-functional interpretation.[5] "Elasticity" thus describes "how" computing resources are expanded.

The term is closely linked with scalability and refers to the ability of a service to adjust computing resources to changing usages above all in an **automated, rapid and dynamic manner**. Elasticity is therefore the contractually based process within the service by which the scalability mechanisms are implemented. In practice this is a very variable procedure depending on the individual service and the underlying contractual requirements (eg the addition of vCPUs, RAM or instances/container instances and pods for containerisation).

Elasticity thus describes the ability not only to expand resources but to do so **virtually in real time** or at least at short notice and to reduce them again just as swiftly when the need no longer exists, depending on requirements. Elasticity is frequently characterised by the adjustment being carried out without any manual outlay worth mentioning and in many cases in a rule-based manner. This can therefore take place both automatically and on demand. An elastic service should ultimately supply the requisite capacity without holding excess capacities permanently in reserve and thereby facilitate an efficient use of resources. It comprises both continuous (automatic) and discrete (on-demand) expansion. Elasticity thus primarily has vertical significance (performance per instance).

Elasticity can accordingly be measured on the basis of both the temporal component for scaling performance up or down and the efficiency of supply (this includes the share of reserve capacities held to avoid reaching a capacity limit). As this depends on the contractual requirements, the corresponding foundation must be assessed when determining whether or not a service is elastic.

Some literature sources therefore consider this feature to offer an opportunity for services to "remove themselves by definition" from the scope of application of the norm.[6] However, this must be countered by pointing out that there is no strict guideline for the degree of elasticity, meaning that the concept is to be interpreted broadly in a customer-friendly manner and to this end the existence of a corresponding business model already suffices. A time delay preconfigured by the provider in the provision of computing resources does not serve to eliminate it from the scope of application. Individual agreements of the service provider with customers that run contrary to the actual business model also do not mean that the service is no longer to be considered elastic. However, a review must be conducted on a case-by-case basis as to whether elastic computing resources exist.

According to the wording, configurable, scalable and elastic computing resources are required to fulfil the present legal definition. This means that it must be possible not only

5 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
6 Freiberg/Niebuhr, BB 2025, 1067 (1069); Siglmüller, MMR Beil. 2024, 112 (114).

to expand computing resources horizontally for a large number of customers, but also to do so flexibly and at short notice for individual customers, even if the individual customer does not perceive this (contractually).

***Examples*:** auto-scaling, serverless computing (on request), Horizontal Pod Autoscaling, automatic increase/reduction of database read replicas, content delivery network (CDN)-assisted traffic peak load distribution.

Positive delineation: data processing services are elastic that enable computing, storage or network resources to be expanded or reduced rapidly according to needs within the scope of a contractual and technical overall perspective. A service is particularly considered to be elastic if it permits a short-term and dynamic scaling of resources both upwards (expansion) and downwards (scale-down).

***Negative delineation*:** a service that altogether does not allow for any short-term and dynamic scaling is not elastic.

- **computing resources** (German: Rechenressourcen; French: essources informatiques; Spanish: recursos informáticos)

The Data Act does not contain any legal definition of the concept of computing resources. However, the term is generally applied within the scope of cloud services and refers to the available **IT capacities** provided for data processing, such as computing power, storage and network performance.

The term “computing resources” is thus the generic term for the underlying physical and logical **IT components** required to store, process and transfer data. The resources are **provided as a service by a corresponding service provider** without the need for customers to acquire their own hardware. They typically include the following basic components: processing performance (CPU) to enable data processing to take place, random access memory (RAM) to facilitate rapid data processing, network bandwidth/network performance or network storage (recital 80 sentence 3) for transmitting and receiving data, storage space (server/SSD)/storage capacity for storing data permanently or temporarily. Recital 80 sentence 2 particularly includes “resources such as networks, servers or other virtual or physical infrastructure, software, including software development tools, storage, applications and services” as computing resources. In addition, recital 80 sentence 3 refers to server time as part of computing resources. However, raw data to be processed by these computing resources cannot be subsumed under the term as they do not comprise an infrastructure resource.

These components are kept on hand individually or coupled with other components by the service provider and provided to customers flexibly in line with their needs via the internet.

***Examples*:** virtual machines (VMs), ie allocated CPUs and storage capacities, storage space for files, databases and backups. CPUs for big data analyses, database instances, ie storage and computing power combined with other services if applicable, software (including software development tools).

***Negative delineation*:** components not belonging to the necessary technical infrastructure: purely legal services (contract consulting), customer advice and incident hotline, advisory services and support with establishing management processes (training for internal organisational and legal processes), pure software licences, supplementary services such as auditing, reports, marketing support, data.

- **of a centralised,** (German: zentralisierter; French: de nature centralisée; Spanish: de carácter centralizado)

The term “centralised” is frequently used in the context of digital infrastructures and cloud architectures and describes data processing for which computing resources and management functions are essentially bundled **at a central location** or within a **centrally managed environment**.

“Centralised” is thus a generic term for IT architectures in which the storage, processing and administration of data largely take place at a **central data centre,** a **central cluster** or a **uniform platform**. Management (eg provisioning, monitoring, authorisation management) is typically organised via central components. By contrast, peripheral terminal devices primarily serve as access points to central data storage. Central provision can take place physically (a location/data centre) or logically (a central tenant/cluster in a cloud region). The key factor is that the relevant computing and management functions are not spread across multiple independent nodes but remain centrally bundled.

***Examples*:** central data centre of a company (on-prem), central cloud tenant in a region, central database instance as single primary system, central application server with central user administration.

***Negative delineation*:** architectures for which computing and data processing are permanently spread across multiple autonomous locations/nodes (eg edge computing with local processing, peer-to-peer structures with no central management instance) are not centralised.

- **distributed or** (German: verteilter oder; French: distribuée ou; Spanish: distribuido o)

For practical purposes, “distributed” refers to a form of architecture for which computing resources, data storage and processing functions are distributed **across multiple systems, locations and nodes** and do not converge exclusively in a central unit. Recital 80 sentence 7 defines distributed computing resources as those that “are located

on different networked computers or devices and which communicate and coordinate among themselves by message passing".

"Distributed nature" therefore describes IT systems in which components of data processing (eg computing, storage, databases, services) are physically or logically distributed **across multiple units**. The objective in many cases is to achieve enhanced reliability, improved scalability, lower latency or load distribution. Communication takes place via networks; coordination can be configured centrally (orchestration) or decentrally (consensus mechanisms).

It is not imperative for classification as "distributed" for all components to be peripheral. It frequently suffices for crucial processing steps or databases no longer to be bundled in just a single system but spread across multiple instances.

***Examples*:** cluster operation of an application across multiple servers, distributed database (replication/sharding), microservices architecture, content delivery networks (CDN).

***Negative delineation*:** a system is not "distributed" if functionally it is fully operated on a single server or in a single instance, even if users access it from different locations (see above under "centralised").

- **highly distributed nature** (German: hochgradig verteilter Art; French: fortement distribuée; Spanish: muy distribuido)

The expression "highly distributed computing resources" is used in the cloud and infrastructure context to describe systems that are not only distributed, but operated to a special degree **across a very large number of nodes, locations or zones** and therefore manifest pronounced decentralisation of data processing. Recital 80 sentence 8 defines highly distributed data processing services as those "that involve data processing closer to where data are being generated or collected, for instance in a connected data processing device".

"Highly distributed nature" thus refers to architectures where the processing and/or storage of data is distributed on a large scale across multiple instances, frequently scaled dynamically and in many cases broadly rolled out geographically. A characteristic feature is that the failure of individual nodes often does not cause any relevant system failure as redundancy, replication and automated backup mechanisms are structurally provided for. Such systems are typically designed to ensure elasticity, fault tolerance and global availability. The term thus refers to an enhanced form of distribution where decentralisation not only encompasses "multiple servers" but also a system design that facilitates operation across a large number of units. Recital 80 sentence 8 describes edge computing as a form of such highly distributed data processing.

***Examples*:** globally distributed cloud platforms with multi-region architecture, distributed object storage systems with automatic replication across zones/regions, edge computing

networks where data processing takes place close to the terminal device, globally distributed CDN infrastructure.

***Negative delineation*:** systems are not highly distributed that are redundant (eg active-passive) or reflected across a few locations but essentially remain dependent on a small number of central components. Architectures for which distribution only exists as a backup or emergency solution, but not as a regular operating model, also do not count.

By defining central, distributed and highly distributed computing resources, the legislator displays its intention of covering every corresponding form of technically implemented computing resource, from central services via a data centre to edge computing solutions.

- **and that enables** (German: ermöglicht; French: et qui permet; Spanish: y que permite)

“Enable” means here that the provision of computing resources **is potentially implementable from a technical perspective.** Service providers must accordingly lay the technical foundations to enable the customer to **use** the resources (eg through activation and access via portal/API). Whether the customer actually does use the resources is irrelevant. The same also applies if the service fails to work in individual cases.

- **with minimal management effort** (German: die mit minimalem Verwaltungsaufwand; French: libérées avec un minimum d'efforts de gestion; Spanish: que con un mínimo esfuerzo de gestión o)

The requirement that only minimal management effort may be entailed by the provision or enabling of a corresponding service makes clear that only those services are to be included that are easy to manage. “Minimal” refers here to the technical outlay and the associated investment of time and staff (eg for interactions and coordination). This requirement is typically met by a digital service with a high degree of automation, thus rendering self-imposed internal release processes for individual customers superfluous.

This component of the definition primarily addresses the effort on the customer side. The customer must be able to initiate, expand, amend and terminate the resources swiftly and unilaterally; see recital 80 sentence 3. This particularly includes services for which no time-consuming adjustments are necessary, thanks to the possibility of auto-scaling, for example. The customer should consequently incur as little organisational and administrative work to use the service as possible. This applies to both the staff and the time outlay for operation, configuration and maintenance.

The decisive factor in this respect is the outlay during operation and not any potentially higher outlay for initial configuration or data migration.

***Examples*:** no time-consuming manual administration for permanent server maintenance, option of using automated processes (eg for scaling, updates, monitoring), standardised administration via APIs or (user-friendly) portals.

***Negative delineation*:** no standardised digital service but modular solutions. Joint design of an individual architecture/integration solution. Customer must develop complex dependencies by itself (eg backup solutions, monitoring etc.). Significant outlay for operation, updates or patching must be met by the customer.

- **or service provider interaction** (German: oder minimaler Interaktion des Diensteanbieters; French: et ou d'interaction avec le fournisseur de services; Spanish: interacción con el proveedor de servicios)

In addition, corresponding services are included that customers can provision, expand at short notice or release with **minimal or even no interaction with the service provider**; see recital 80 sentence 3. This component of the definition therefore conversely relates to the effort on the provider side.

What is meant is that the customer can largely utilise, adjust and manage the computing resources **independently** without the need for any **manual intervention** by the provider or individual coordination. This comprises specific, pre-packaged combinations of ICT resources that do not have to be developed individually; see recital 81 sentence 3.

Example: provisioning by the customer without manual intervention by the provider by means of automation or self-service, release processes in the form of deletions and deactivations can also be initiated independently by customers without the need for any time-consuming manual technical implementations.

***Negative delineation*:** many manual processes such as inbuilt provisioning only pending ticket/request, manual release processes, manual configuration of service for each customer (eg individual set-ups instead of templates), individual integration work at customer end necessary, resources are not available on a pool-based manner but bilateral capacity planning required. Cloud management and Security as a Service solutions frequently require “more than just minimal interaction of the provider” at present.[7]

- **rapidly provisioned and** (German: rasch bereitgestellt und; French: qui peuvent être rapidement mobilisées; Spanish: y liberarse rápidamente)

A provisioning of computing resources (see above) means that they already exist and can theoretically be utilised and merely need to be made available to the customer practically, for instance by setting up an account or allocating resources. This requirement

7 Sattler, CR 2024, 213 (215).

pertains to the short-term availability of a server, a virtual machine or the provisioning of storage space.

The resource is made available rapidly if this takes place on a short-term basis, generally within a few minutes or hours. A changeover lasting several weeks can no longer be considered rapid. This requirement pertains merely to the time needed for the technical changeover, not to the practical execution time that may take longer due to other criteria (eg contractual negotiations).

Altogether, this requirement only concerns the technical possibility and not the actual implementation (cf. the verb “can”).

***Examples*:** VM/server is created, storage is created, configuration of a database instance, service is configured and activated.

***Negative delineation*:** individual programming of a customer requirement previously reported

- **released** (German: freigegeben werden können; French: puede movilizarse).

As well as making computing resources available, their rapid deactivation or deletion (deprovisioning) is also cited as a criterion. The release of resources accordingly refers to the technical possibility of terminating at short notice the computing resources provided for (individual) customers, for instance because the requirement in question no longer exists. A technical possibility to reduce resources at short notice is therefore also required in this connection.

The sole decisive factor here is the technical possibility and not its actual implementation (cf. the verb “can”).

***Examples*:** reduction of instances through auto-scaling, test server/database is swiftly deleted after the end of a project, containers are automatically removed, database instances are shut down.

***Negative delineation*:** single components of a cloud service are individually removed for one customer in a time-consuming procedure. Use only according to custom integration (eg IAM concept at customer end, specific employees of the customer are removed individually for this customer and a corresponding service is reconfigured in a time-consuming procedure).

2.1.2 Supplementary (overall) assessment

The regulatory body has decided for the first time to provide its own legal definition of the term “data processing service” in the Data Act. While in the Regulation on a framework for the free flow of non-personal data in the European Union it defines the data processing service via the service provider (Article 3(4) of the Regulation on a framework for the free

flow of non-personal data in the European Union), the Data Act draws on the service's technical functionalities. The newly created definition and recital 80 f. intended to specify it more precisely build on the definition of cloud computing by the US National Institute of Standards and Technology (NIST) of 2011 but are not to be considered identical.[8] Notwithstanding the fact that many of the requirement features are taken from a technical standard, the definition here is not to be interpreted purely technically but in contractual functional terms.[9]

Recital 81 sentence 1 describes the concept of "data processing services" as covering "a substantial number of services with a very broad range of different purposes, functionalities and technical set-ups". The aforementioned requirements are therefore to be interpreted broadly and the complexity and type of data processing services can vary considerably; see recital 87 sentence 1. At least services such as "Infrastructure as a Service" (IaaS), "Platform as a Service" (PaaS) and "Software as a Service" (SaaS) models[10] therefore fall under this concept; see recital 81 sentence 2. However, this designation is not to be considered exhaustive, as other provisioning models, such as "Storage as a Service", "Database as a Service", "AI as a Service"[11] and other as-a-service products (XaaS) etc. as well as hybrid forms and package solutions can also be covered by it; see recital 81 sentence 4. It is irrelevant here if the service provider offers additional software solutions to the aforementioned services that are based on the corresponding models but do not themselves fully meet the aforementioned requirements. Moreover, cloud and edge services also belong to the scope of application of this definition; see recital 78 sentence 1. However, a careful examination must be carried out for pure edge services as data processing here takes place close to the source of generation, such as an IoT device. The underlying edge computing infrastructure may provide for data processing on the device itself for which the necessary flexibility for fulfilment of the requirement such as configurability, scalability and elasticity may not exist.[12] However, these infrastructures are partly also integrated in cloud solutions.[13]

It is not ultimately the designation of the data processing service model that counts but rather a review is needed in individual cases of the aforementioned requirements. Other IT services that do not fall in the aforementioned categories can therefore also be subsumed under the definition.

---

8 NIST, *The NIST Definition of Cloud Computing*, Special Publication 800-145, September 2011, pp. 1, 2 et seq. See also Siglmüller/Zdanowiecki, RDi 2025, 504 (505); Niebuhr K&R 2025, 361 (362); Pommerening/Nickel RDi 2024, 289 side note 9; Siglmüller MMR 2024, 112 (114).

9 For a detailed discussion of the difference between a technical and a contractual-functional interpretation, see Siglmüller/Zdanowiecki, RDi 2025, 504 (506).

10 However, this may not apply to Application Service Providing (ASP); cf. Siglmüller/Zdanowiecki, RDi 2025, 504 (510).

11 Sattler, CR 2024, 213 (215).

12 Schreiber/Pommerening/Schoel *Der neue Data Act* Art. 6 side note 28 et seq.

13 Schreiber/Pommerening/Schoel *Der neue Data Act* Art. 6 side note 29; Pommerening/Nickel RDi 2024, 289 side note 11.

Data processing services within the meaning of Article 2(8) of the Data Act are primarily used in the B2B sector.[14]

Not all the features mentioned must be fulfilled by the service provided.

The following requirements must be met cumulatively:

1) digital service,
2) customer,
3) ubiquitous,
4) on-demand network access,
5) shared pool,
6) configurable,
7) scalable,
8) elastic,
9) computing resources,
10) rapid provisioning,
11) rapid release.

The service must alternatively also:

12) be centralised, distributed or highly distributed and
13) be capable of being provisioned or released with minimal management effort (for the customer) or minimal service provider interaction.

However, it is not also necessary for use actually to be made of this in every contractual relationship. The existence of the technical possibilities fundamentally suffices in itself. Furthermore, (temporarily provisioned) test and evaluation versions can also be covered by the legal definition of the data processing service a contrario Article 31(2) of the Data Act (it would otherwise not have been necessary for them to be excluded from the scope of application by Article 31(2) of the Data Act). In particular, the labelling of a digital product as a beta version does not exempt it from fulfilment of the criteria of the legal definition.[15] An overall assessment of the service is required in borderline cases.[16] However, the hardware infrastructure is of subordinate importance here.[17]

Data processing services covered by Article 2(8) of the Data Act are cited in the literature particularly to include the following: Compute & Storage (eg Google Cloud Engine, Microsoft Blob Storage), Software as a Service with sizing by the customer (eg SAP RISE).[18] However, the private cloud poses a borderline case as it comprises different configuration options so that it comes down to the individual case. Virtual private clouds can for the most part be classified as data processing services, in contrast, for example,

14 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
15 Freiberg/Niebuhr, BB 2025, 1067 (1069).
16 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
17 Freiberg/Niebuhr, BB 2025, 1067 (1068).
18 Siglmüller/Zdanowiecki, RDi 2025, 504 (509 et seq.).

to physical (separated) private clouds. This is because virtual private clouds are frequently based on the same jointly used physical infrastructure as public cloud environments and only differ by way of a logical client separation at the network and access level. The underlying computing resources therefore continue to originate from a centrally managed, scalable resource pool that fulfils typical cloud properties such as scalability and elasticity. By contrast, purely physically separated private cloud infrastructures frequently manifest a fixed capacity commitment and restricted elasticity and are thus closer to typical dedicated data centre solutions. Hybrid solutions in particular need to be considered on a case-by-case basis.[19] This can also include email services with a selection of different storage options.[20]

In addition, not all the requirements must be met by a provider itself. Instead, individual components of the service can also be provided by third parties.[21] However, they must be attributable to the provider, for instance because the latter has a contract with the customer regarding the provisioning of the corresponding service. Some also consider that the customer must benefit from this service.[22] However, this view goes too far as it is also intended to apply to a service provider who provides a corresponding service and fails at times to fulfil all the requirements due to service malfunctions. Customers who then switch service should not find themselves worse off as a result.

The service provider of the data processing service is the contracting partner of the customer. In the event of a (genuine) reselling offer, the requirements for the existence of a data processing service apply to the reseller.[23]

2.1.3 Services not included

Nevertheless, it is not sufficient for fulfilment of the understanding of the concept for any random digital service to be operated via an infrastructure service operated via a third party (such as a cloud service), ie for it to make use of network access to a shared pool of configurable, scalable and elastic computing resources without this being part of the contract between the customer and the service provider to qualify as a data processing service within the meaning of Article 2(8) of the Data Act.[24] Although the broad wording of Article 2(8) of the Data Act also does not rule out such an interpretation, these cases are not to be included.[25] However, the digital service in this case does not allocate any computing resources, but merely makes use of predefined functionalities (eg bird voice apps, training apps and social media apps for which not the computing power is paramount but interaction with others and messenger applications).[26] The inclusion of

19 Against inclusion in the scope of application as the authors consider there not to be sufficient flexibility owing to the limited volume sizes (eg 1 GB and 5 GB), Siglmüller/Zdanowiecki, RDi 2025, 504 (511). This view is not shared here. There is no requirement for the option of adding unlimited storage space.
20 Siglmüller/Zdanowiecki, RDi 2025, 504 (509 et seq.).
21 This issue is raised by Bomhard MMR 2024, 109 (110).
22 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
23 Siglmüller/Zdanowiecki, RDi 2025, 504 (512).
24 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
25 For a convincing argument, see Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
26 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).

such services by Article 23 ff. of the Data Act would in most individual cases lead to results that were difficult to justify [27] and be virtually impossible as the providers of such services cannot exert any influence on the cloud service provider whose services they themselves procure as customers. If the service offered could also have been provided via a server with fixed computing resources and the service provider has only opted for a third-party cloud provider for reasons such as cost, availability or IT security, the customer is not entitled to any further rights in this contractual relationship from Article 23 ff. of the Data Act, especially as this digital service does not facilitate for the customer ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or minimal service provider interaction. Instead, the service in question is one that merely happens to be operated on this virtual infrastructure covered by Article 2(8) of the Data Act. In some cases, the customer/user of such a service will not even be aware of the environment in which this service is operated.[28] It would be unfair if the customer of this service were now to have other rights merely based on the provider's choice of infrastructure despite himself not being able to make any direct use of the benefits or functions resulting from the criteria set out in Article 2(8) of the Data Act. There are also no significant lock-in effects and switching or market entry barriers in this respect that the regulatory body wished to address with this regulation.[29] By the same token, however, the provider of this service could assert its rights from Article 23 ff. of the Data Act with regard to its infrastructure provider. This can only not be the case if the provider of this service is itself also the operator of the infrastructure solution and the associated operational features are also contractually agreed with the customer and the service is only an additional functionality (eg a meeting tool or the like).

Concerning the aforementioned requirements, the service must be capable of actually ensuring their technical fulfilment. If this is not the case but a company nevertheless advertises compliance with said requirements (cloud washing), this can have various legal consequences. These range from infringements of the Act against Unfair Competition and potential revocation of a contract concluded on the basis of the advertising message through to possible accusation of fraud.

However, this does not mean that a service that does not actually fulfil the requirements of Article 2(8) of the Data Act and merely claims to do so for advertising purposes falls within the scope of application of this norm or is required to meet the associated obligations for data processing services for this reason alone. Excessive marketing does not therefore justify application of the provision. Nevertheless, the company advertising bears the burden of proving to the supervisory authority that the case in question merely concerns an advertising message without substance.

27 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).
28 Siglmüller/Zdanowiecki, RDi 2025, 504 (506, 512).
29 Siglmüller/Zdanowiecki, RDi 2025, 504 (506).

Purely on-premise solutions are generally not classified as data processing services for lack of scalability and elasticity as well as a shared pool of computing resources.[30]

Pure hosting providers in the narrower sense (providers of storage space, ie "infrastructure, technology and/or maintenance required for the storage, provisioning and management of applications, websites or data on servers"[31], without the ability to access other resources according to need and transfer data to other servers or the like) are not considered in the literature to be data processing services.[32] National implementation of the NIS 2 Directive explicitly excluding website hosting services in its wording is sometimes drawn on here as an argument as there is frequently no scalability and elasticity.[33] However, this apodictic view is not necessarily convincing and the individual case and overall package associated with the service should instead be considered.

Some edge services only process data locally on the corresponding device or in a nearby edge infrastructure without the data being linked via a cloud solution. These edge services are not to be considered data processing services but are more akin to pure hosting services (see above).[34] These services in most cases also lack a shared pool of computing resources.[35] An case-by-case review under consideration of the underlying architecture is therefore required in particular for edge services.[36]

Pure telecommunication services that merely convey data[37] and online search engines are indisputably not to be considered data processing services as customers/users consistently have no configuration option here.[38]

Managed services for cloud and edge services of third parties tasked with supporting customers in the management of their on-premise resources (eg databases or applications) should likewise be excluded. The authors believe that this is justified by the fact that the objective of Chapter VI cannot be pursued further here as the data are already on-prem with the customer.[39] The same applies to Software as a Service on the basis of dedicated infrastructure (ie Application Service Providing (ASP)).[40] The possibility of scalability and rapid provisioning and release is usually lacking here.

Also not included are products that have been developed individually for a customer so that these computing resources are not offered to other customers via a pool and

---

30 Schreiber/Pommerening/Schoel, *Der neue Data Act* Art. 6 side note 33.
31 Freiberg/Niebuhr, BB 2025, 1067 (1068).
32 Monschke/Lück in: Paschke/Schumacher, *EU Data Act*, Art. 2 side note 69; Weinhold, in: Geminn/Johannes, *Europäisches Datenrecht*, Art. 26 side note 11, Schreiber/Pommerening/Schoel *Der neue Data Act* Art. 6 side note 27; Pommerening/Nickel RDi 2024, 289 (291) side note 12.
33 Siglmüller/Zdanowiecki, RDi 2025, 504 (506, 509).
34 Schreiber/Pommerening/Schoel, *Der neue Data Act* Art. 6 side note 29 et seq.
35 Schreiber/Pommerening/Schoel, *Der neue Data Act* Art. 6 side note 31.
36 Pommerening/Nickel, RDi 2024, 289 side note 11; Schreiber/Pommerening/Schoel, *Der neue Data Act* Art. 6 side note 32.
37 Siglmüller/Zdanowiecki, RDi 2025, 504 (512).
38 Weinhold, in Geminn/Johannes, *Europäisches Datenrecht*, Art. 26 side note 13.
39 Siglmüller/Zdanowiecki, RDi 2025, 504 (509).
40 Freiberg/Niebuhr, BB 2025, 1067 (1068 f.); Siglmüller/Zdanowiecki, RDi 2025, 504 (510). Pommerening/Nickel, RDi 2024, 289 (291) side note 13.

therefore also not scalable with minimal management effort (see recital 98 sentence 1).[41] So-called “custom-built” solutions, ie the development and provisioning of individual software, generally therefore fall under this. However, it is not the degree of individualisation of the application that is decisive in borderline cases, but the technical structure of resource use. Pool-based, auto-scalable services speak in favour of a data processing service, while dedicated and manually operated individual solutions speak against this. It is for this reason that a case-by-case review is also required here as there may also be corresponding services that nevertheless count as data processing services. Were this not to be the case, the regulatory body would not have enacted the provision of Article 31(1) of the Data Act.

Examples: A company in a highly regulated sector, such as the financial/insurance sector, has a platform developed by a cloud provider that is specially tailored to regulatory requirements. The application is individually programmed from a functional perspective (own workflows, special compliance modules). However, this platform is operated entirely on the provider’s standardised cloud infrastructure. The underlying computing resources come from a shared compute and storage pool, are provisioned automatically, elastically scaled and can be controlled by the customer itself via a portal. Despite the customer-specific configuration of the platform, a data processing service within the meaning of Article 2(8) of the Data Act exists due to the cloud components as the pooling of computing resources, on-demand provisioning and configurability, scalability and elasticity requirements are fulfilled. Corresponding providers should therefore carefully review their business models to determine whether the development costs of their (individual) software solutions are expressed sufficiently independently or so far subject to recouping via a lock-in effect of the cloud service also offered that is factored in in advance. The latter in particular can no longer be reliably applied in this form under the provisions of the Data Act. Without the cloud component, the aforementioned software developer would not be considered to provide a data processing service for the developed platform, which in this case would be hosted by the contracting company itself on premise. The fact that the development of the software solution is only of secondary importance for classification as a data processing service and the decisive factor instead comprises the computing resources behind this is reflected in the discussions concerning the reform of the Data Act with the Digital Omnibus package. The intention here is actually to tone down the “custom-build” requirement to “custom-made”, ie a parametrisation rather than an individual development.

It can be inferred from the legal history that online content services such as linear television and non-linear music and video streaming services do not fall within the scope of application of data processing services.[42] See also recital 16, according to which corresponding textual, audio and audiovisual content often covered by intellectual

41 Veil, in BeckOK DatenschutzR/Veil DA Art. 1 side note 109.

42 Lienemann in: HEKLW, *Data Act: An Introduction*, p. 182 et seq. with reference to the Max Planck Institute for Innovation and Competition, Position Statement, 2022, p. 62 para. 170; Geiregat, *The Data Act: Start of a New Era for Data Ownership?* 2022, pp. 30 et seq at para. 31; Commission, COM(2022) 68 final p. 39.

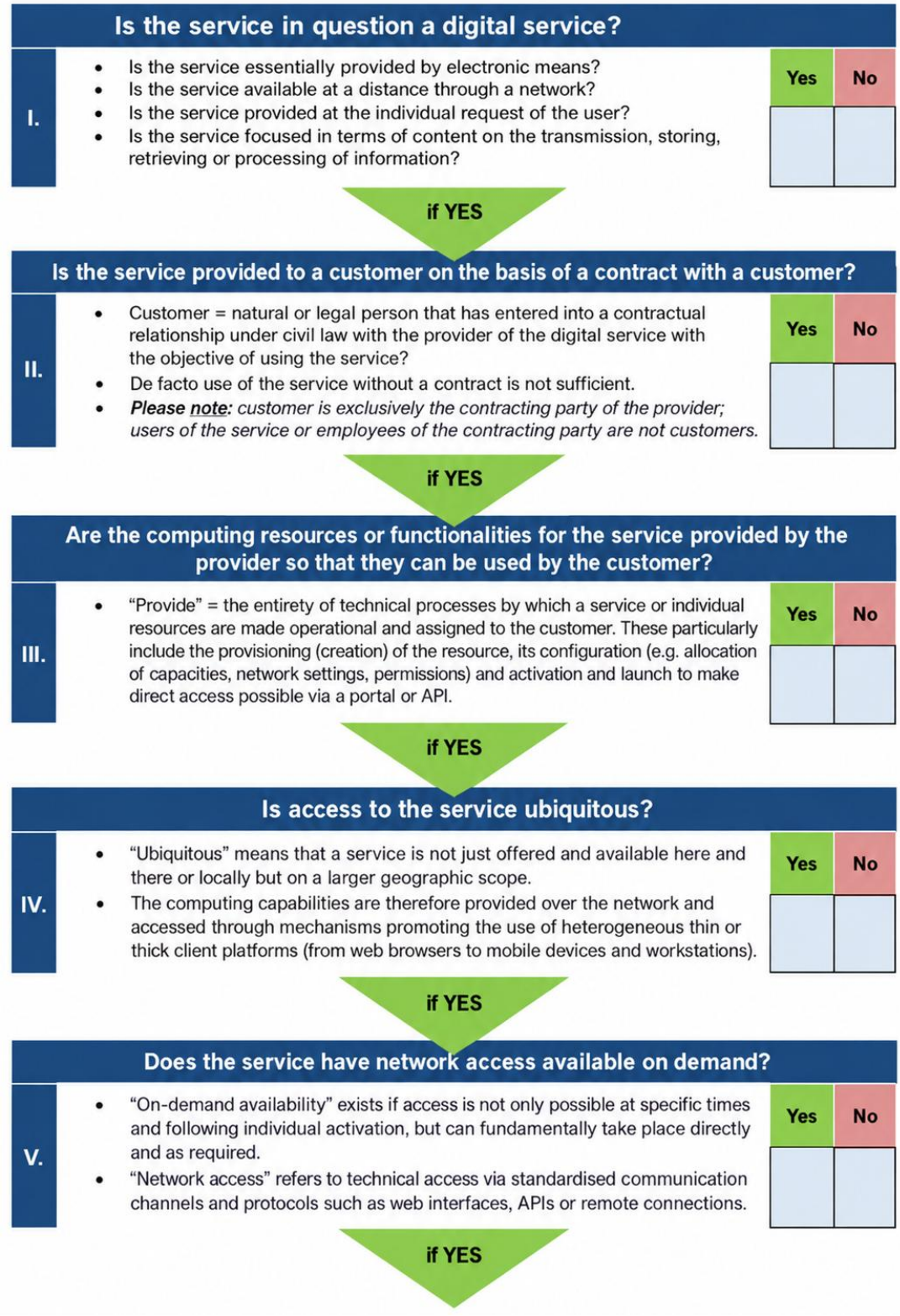
property rights is to be distinguished from the scope of application of the Data Act.[43] Video-on-demand services are therefore not included here.[44]

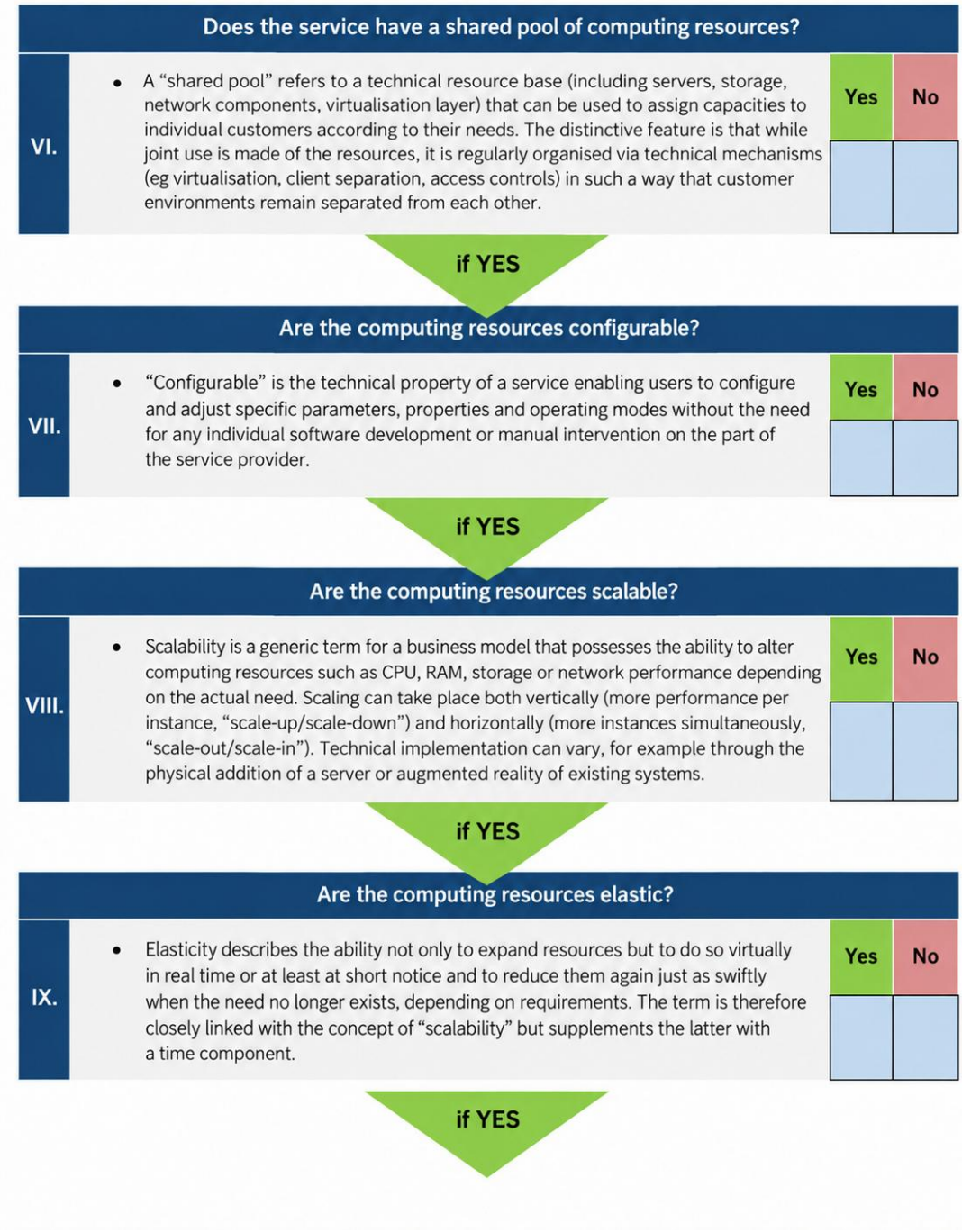
2.2 Development of the assessment framework for identifying data processing services

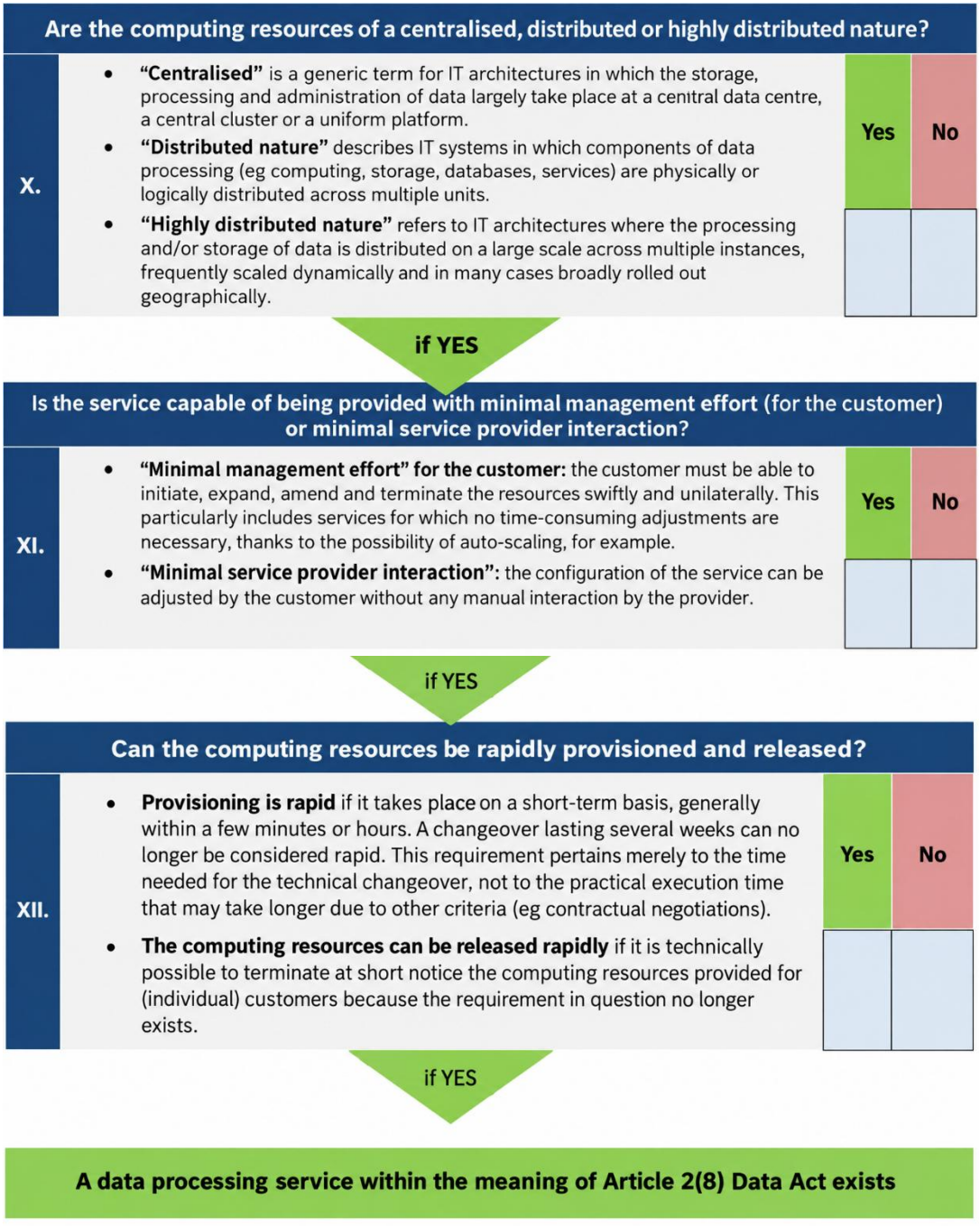
Based on the legal assessment in the previous paragraph, the following assessment framework has been drawn up with categories that are verifiable and resilient from a technical and legal perspective. If all 12 assessment categories can be answered positively, a data processing service within the meaning of Article 2(8) of the Data Act exists.

43 Monschke/Lück in: Paschke/Schumacher, *EU-Data Act*, Art. 2 side note 69; Lienemann in: HEKLW, *Data Act: An Introduction*, p. 183.
44 Piltz/Zwerschke, CR 2024, 153 (154), KOM FAQ Data Act Version 1.4 para. 58a.

Figure 2-1: Data processing service assessment framework




Does the service have a shared pool of computing resources?
VI.
A "shared pool" refers to a technical resource base (including servers, storage, network components, virtualisation layer) that can be used to assign capacities to individual customers according to their needs. The distinctive feature is that while joint use is made of the resources, it is regularly organised via technical mechanisms (eg virtualisation, client separation, access controls) in such a way that customer environments remain separated from each other.
Yes
No
if YES
Are the computing resources configurable?
VII.
"Configurable" is the technical property of a service enabling users to configure and adjust specific parameters, properties and operating modes without the need for any individual software development or manual intervention on the part of the service provider.
Yes
No
if YES
Are the computing resources scalable?
VIII.
Scalability is a generic term for a business model that possesses the ability to alter computing resources such as CPU, RAM, storage or network performance depending on the actual need. Scaling can take place both vertically (more performance per instance, "scale-up/scale-down") and horizontally (more instances simultaneously, "scale-out/scale-in"). Technical implementation can vary, for example through the physical addition of a server or augmented reality of existing systems.
Yes
No
if YES
Are the computing resources elastic?
IX.
Elasticity describes the ability not only to expand resources but to do so virtually in real time or at least at short notice and to reduce them again just as swiftly when the need no longer exists, depending on requirements. The term is therefore closely linked with the concept of "scalability" but supplements the latter with a time component.
Yes
No
if YES


Are the computing resources of a centralised, distributed or highly distributed nature?
X.
"Centralised" is a generic term for IT architectures in which the storage, processing and administration of data largely take place at a central data centre, a central cluster or a uniform platform.
"Distributed nature" describes IT systems in which components of data processing (eg computing, storage, databases, services) are physically or logically distributed across multiple units.
"Highly distributed nature" refers to IT architectures where the processing and/or storage of data is distributed on a large scale across multiple instances, frequently scaled dynamically and in many cases broadly rolled out geographically.
Yes
No
if YES
Is the service capable of being provided with minimal management effort (for the customer) or minimal service provider interaction?
XI.
"Minimal management effort" for the customer: the customer must be able to initiate, expand, amend and terminate the resources swiftly and unilaterally. This particularly includes services for which no time-consuming adjustments are necessary, thanks to the possibility of auto-scaling, for example.
"Minimal service provider interaction": the configuration of the service can be adjusted by the customer without any manual interaction by the provider.
Yes
No
if YES
Can the computing resources be rapidly provisioned and released?
XII.
Provisioning is rapid if it takes place on a short-term basis, generally within a few minutes or hours. A changeover lasting several weeks can no longer be considered rapid. This requirement pertains merely to the time needed for the technical changeover, not to the practical execution time that may take longer due to other criteria (eg contractual negotiations).
The computing resources can be released rapidly if it is technically possible to terminate at short notice the computing resources provided for (individual) customers because the requirement in question no longer exists.
Yes
No
if YES
A data processing service within the meaning of Article 2(8) Data Act exists

2.3 Limits of the assessment framework and consequences resulting from them

2.3.1 Structural scope for interpretation of the legal definition

Functional-technical vs. contractual-functional interpretation

One fundamental scope for interpretation arises from the dual structure of the legal definition: it draws on the one hand on technical properties (eg scalability, elasticity, pooling) and on the other hand on contractual relationships (eg customer, provisioning). This interlacing necessitates a “contractual-functional interpretation”. Both technical and contractual criteria must be considered in the norm interpretation. A grey zone arises here in practice above all if technical capabilities exist but are not agreed or are even excluded contractually. The reading of the legal definition chosen here makes clear that the technical possibility already suffices in itself, regardless of any actual use. This simultaneously opens up scopes for interpretation regarding the question of the extent to which “potential functionality” can suffice. It remains unclear whether latent technical properties without contractual operationalisation are always sufficient or whether a given degree of functional accessibility must be required. A further challenge exists if the technical requirements are met but are technically restricted or overcomplicated in such a way (technical possibility of automation but a human must actively release computing resources) as to circumvent the application of the Data Act (eg in terms of the scalability of computing resources and the minimal management effort or minimal service provider interaction).

Broad interpretation vs. normative limitation

The legal definition is deliberately broadly formulated in various places to include a “significant number of services”. At the same time, it contains implicit limitations owing to the large number of requirements to be met. This gives rise to tension as to how broadly individual components of the legal definition are to be interpreted. This tension leads to grey zones in particular for digital platform services and SaaS applications if these are based on cloud infrastructure but the customer is not granted any direct control over computing resources.

2.3.2 Grey zones and borderline cases

There are various borderline cases in practice as technical architectures are often not transparent. They can also change dynamically, thereby impeding ex-ante classification for a supervisory authority.

Hybrid service models

Hybrid architectures represent a core borderline case for data processing services. They combine cloud-based resources with local or edge-like components. Challenges can arise here from local components not being scalable or the rejection of a pooling of computer resources. Despite the many different criteria, an overall assessment is required for application of the legal definition. Data processing can take place locally without entirely fulfilling the typical cloud properties particularly in the case of edge computing.

Partly standardised services

A further grey zone concerns partly standardised services consisting of modular components. The question arises here as to whether the service is provided “with minimal management effort” or already falls within the scope of individual project services. The distinction between configuration (permissible within the definition) and individual development (essentially not covered) can prove blurred in practice.

Customer-specific platform solutions (“custom-build”)

Cases of customer-specific software solutions operated on standardised cloud infrastructure are particularly complex. The legal definition suggests that a data processing service can exist in such cases despite individual software development as long as the underlying computing resources are pooled and meet the specified criteria. Significant scope for interpretation arises here, particularly regarding the question as to the degree of individualisation from which standardisation of the infrastructure is “superimposed”.

Managed services and support services

Managed services for cloud or on-premise systems also constitute borderline cases. They access existing infrastructure but do not themselves provide any computing resources. The decisive factor here is whether the service itself represents a “provisioning” within the meaning of the legal definition or merely fulfils supporting functions.

2.3.3 Addressing of scopes for interpretation

The scopes for interpretation must be addressed by the supervisory authority by way of a multi-level assessment logic.

A key solution approach consists of establishing a multi-level assessment model covering various levels:

1. **Infrastructure level** (the technical components are assessed here: pooling, scalability, elasticity)

2. **Service level** (the functional components are assessed here: provisioning, network access, configurability)
3. **Contractual level** (the contractual elements are assessed here: customer relationship, service content)

Classification as a data processing service should accordingly not take place in an isolated manner but by means of an integrated consideration of all the levels.

In addition, a case-by-case assessment and focal analysis are required for hybrid and mixed services to determine which component shapes the economic and functional main service. A review is also necessary here to establish whether typical cloud properties are formative or only accessory features for the data processing service to be able to assume application of the legal definition for hybrid solutions.

3 Establishment of a classification model for "same service types"

3.1 Structured interpretation of the concept "same service type"

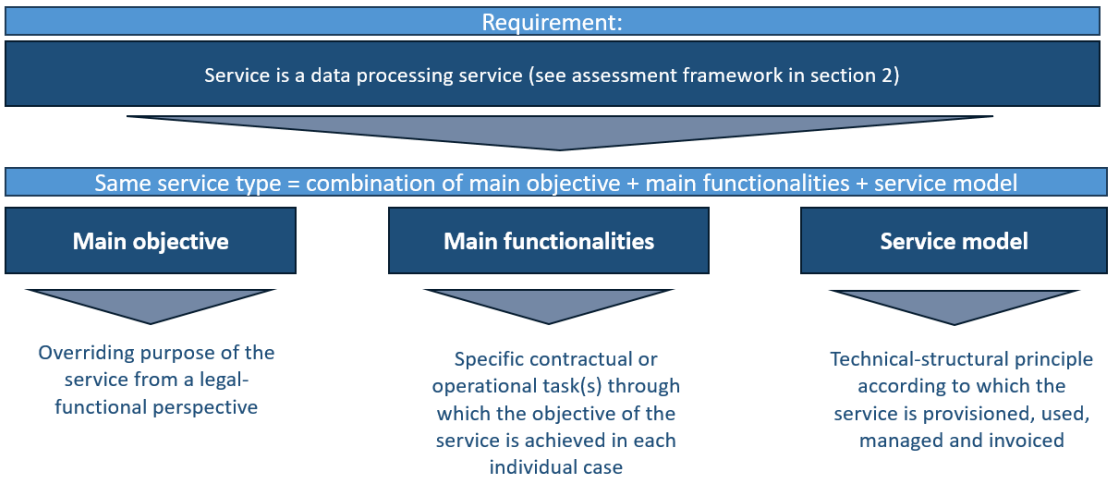
According to Article 2(9) of the Data Act, "same service type" (German: gleiche Dienstart; French: même type de service; Spanish: mismo tipo de servicio) means a set of data processing services (German: eine Reihe von Datenverarbeitungsdiensten; French: un ensemble de services de traitement de données; Spanish: un conjunto de servicios de tratamiento de datos)

- that share **the same primary objective** and (German: die dasselbe Hauptziel haben; French: qui partagent le même objectif principal; Spanish: que comparten el mismo objetivo primario)[45]
- **data processing service model** and (German: dasselbe Dienstmodell für die Datenverarbeitung; French: data processing service model; Spanish: modelo de servicio de tratamiento de datos y)
- **main functionalities** (German: dieselben Hauptfunktionen; French: les principales fonctionnalités; Spanish: funcionalidades principales).

All relevant services must constitute data processing services within the meaning of Article 2(8) of the Data Act (see assessment framework in section 2).

45 The legal literature points out that this legal definition manifests a high degree of legal uncertainty due to the use of a large number of vague legal concepts; see Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 70.

Figure 3-1: Determination of the “same service type”



Source: WIK-Consult

3.1.1 Main objective

The **main objective** of a digital service means that the services are geared to the **electronic provision of an information or data-related service** to the customer on an **on-demand** basis **via network and information systems** and frequently pertain to the **transmission, storage, processing or provisioning of data and information**. This is based on the overriding purpose of the service from a legal-functional perspective.[46]

Typical features of such a main objective are:

1) the **processing of data** (German: die Verarbeitung von Daten), eg compute

The data processing service has the task of processing data algorithmically, that is, performing computing operations such as analysis, transformation, modelling or the execution of workloads (eg virtual machines).

2) the **storage and retrieval of data** (German: das Speichern und Abrufen von Daten), eg storage

The main focus of the data processing service lies in storing data permanently or temporarily and ensuring it is retrievable (eg object storage and blob storage, backup and archiving solutions). Data are processed for supportive purposes at best (eg encryption, versioning). However, this is not the main objective of the service.

3) the **transmission of data** (German: das Übertragen von Daten), eg communication services

46 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 72 talk of a (macro) level.

The service aims to transport data between systems and users. Any storage or processing of the data merely serves the purpose of enhancing transportation (caching, routing) and is not the main objective (eg content delivery network for the delivery of managed contents, managed messaging).

4) **Making available digital functions** (German: Bereitstellung von digitalen Funktionalitäten) e.g. application, platform or analytical services

The core activity here is to provide the user with a ready application or clearly defined function that processes data and delivers results (eg SaaS applications such as customer relation management (CRM) and collaboration tools, managed database services, analytical and transaction tools and platforms). This requirement is not determined by the purpose subjectively intended by the customer but is to be defined objectively.[47]

The same main objective exists if two services are found by evaluation to fulfil the same primary purpose (data storage or processing or transmission or application/function).[48] There are services that can fulfil several of these objectives in a package.

Examination question: Which (overriding) general purpose does this service type serve?

3.1.2 Service model

In the context of digital data processing services, the expression same service model means fundamentally the same type of service provision**,** ie an identical structural principle according to which the service is technically provisioned, used, managed and invoiced. The key factor is therefore the "specific combination of ICT services"[49] . It is not the actual content of the service that is decisive, but merely the underlying model used for making resources and functionalities available to users via networks; see recital 81 sentences 4 and 5. This particularly includes all IaaS services, all PaaS services, all SaaS services and all other aaS services. Furthermore, there can also be services that contain multiple components of aaS services and package solutions that may be identical.

Examination question: How is the service provided? Is it an IaaS service / PaaS service, SaaS service or a new form of provisioning or mixed form?

47 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 72.
48 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 70; BeckOK DatenschutzR/Schmidt-Wudy, *DA*, Art. 23 side note 31 point out that "the same" is to be understood as meaning "identical".
49 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 73; also BeckOK DatenschutzR/ Schmidt-Wudy, *DA*, Art. 23 side note 33.

3.1.3 Main functionalities

In addition to the same main objective and the same service model, data processing services of the "same service type" should also have the same main functionalities. However, notwithstanding the understanding implied by the wording of the definition, services can also only have one single main functionality or multiple functionalities can be combined in one service. For a full switch of service, a same service type must have the same main functionalities as the service to be switched from.

This same main functionality exists if services essentially fulfil the same data-related task even if they are differently configured technically or differently named.[50]

The main functionality describes the specific technical or operational task with respect to the general main objective that an individual task fulfils and through which the objective of the service is achieved in each individual case. Potential examples include object or block storage in the area of data storage, virtual infrastructure such as virtual machines or serverless containers in the area of data processing and dedicated interconnection or VPNs in the area of data transmission. There is also a large number of digital functionalities, eg for databases or data warehouses. Multiple services can have the same main objective but different main functionalities.

Brandt/Schumacher base their determination of the main functionality on the advertising content (eg "software offers all types of text processing, computing resources are based on a given Linux system or a platform offers specific links to configurable services").[51] However, provider-specific characteristics are to be omitted here.[52]

The concept of **functional equivalence** between two data processing services covering the same service type refers to a situation in which two different services ultimately provide the same main functionalities even if they are differently implemented from a technical perspective. Functional equivalence therefore exists if an alternative data processing service provides the same key functional capabilities so that users can replace their existing service without any fundamental change to usage or business processes. It is not identical technical implementation (or an identical service model in the form of SaaS, PaaS and the like) that is decisive, but comparable functionality and availability.

A service is functionally equivalent if it:

- falls in the same category of main objective (eg storage),
- provides the same main functionality,

50 See also Piltz/Zwerschke CR 2024, 153.
51 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 74.
52 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 74 among other things include computing instances in this context.

- facilitates comparable usage by the customer.

Functional equivalence does **not** mean that two services must be identical. Different providers can implement the same functionality via different technical architectures or technologies. For example, a database service can be functionally equivalent even if:

- different database engines are used,
- the internal architecture is designed differently.

The decisive factor is that the customer is able to achieve the same functional purpose with the service.

As well as a full switch to a same service type, according to Article 23 of the Data Act, a "modular switch" is also possible: this means that not only entire data processing services can be switched, but a partial switch at the level of the main functionalities is also possible. See section 3.3 for a detailed discussion.

Examination question: Which specific data-related activities are paramount for the services to be compared?

In Article 32 of the Data Act, the regulatory body makes use of the term main feature (German: zentrale Funktion; French: caractéristiques principales) instead of main functionalities (German: Hauptfunktion; French: principales fonctionnalités). Although this linguistic distinction is also upheld in other language versions, it can be assumed here that the two terms are used synonymously.[53]

3.1.4 Overall assessment

Although the various main objectives, service models and main functionalities have to be operationally identical, these services can differ in various details such as security measures, APIs etc. without any impact on the application of Article 2(9) of the Data Act.

Moreover, additional functionalities do not impede a service from being categorised as the same service type. This depends merely on the focus of the service.

However, pursuant to recital 81 sentence 6, the regulatory body distinguishes between services of the "same service type" and "comparable services". The latter represent a subcategory of a same service type. However, this only applies if a service of the same service type actually exists in the individual case at hand.[54]

According to recital 81 sentence 7, services of the same service type can possess different and competing features. Comparable services not classified as a category of the

53 This essentially also applies to Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 75.
54 Brandt/Schumacher, in Paschke/Schumacher, *DA*, Art. 2 side note 71.

same service type comprise the same model for the provisioning of data processing services (eg SaaS, IaaS, PaaS) and the same main objective (eg processing of data or storage and retrieval of data). However, according to recital 81 sentence 6 they can differ significantly in terms of their (main) functionalities, distribution model and use cases.

3.2 Derivation and operationalisation of suitable classification criteria

The question is addressed below as to which reliable criteria and categories facilitate a consistent and practical classification of different data processing services, in particular with regard to their main objectives, main functionalities and service models and a classification derived from this as “same service type”.

3.2.1 Literature overview

A review was conducted in an initial step to establish whether any attempts at a classification model for determining the same service type within the meaning of the Data Act already exist in the literature. At the time of publication of this study, it can be confirmed that there is no attempt at a classification model in the existing literature that explicitly pertains to determining the same service type pursuant to the Data Act.

Sources can accordingly only be drawn on in the literature that cover a subsection of such a classification. The following three subsections in particular can be distinguished in this respect:

- Studies on the application and understanding of the term “same service type”
- General cloud taxonomies
- Norms and standards with regard to cloud systems and service model

3.2.1.1 Studies addressing the same service type pursuant to the Data Act:

- Schnurr, D. (2022): *Switching and Interoperability between Data Processing Services in the Proposed Data Act*[55]
- Geradin et. al. (2022): *The Regulation of Cloud Computing: Getting It Right*[56]
- Ennis / Evans (2023): *Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence*[57]

---

55 Schnurr, D. (2022). *Switching and Interoperability between Data Processing Services in the Proposed Data Act*. Report by Centre on Regulation in Europe, 22; https://cerre.eu/wp-content/uploads/2022/12/Data_Act_Cloud_Switching.pdf [8 June 2026].

56 Geradin, D., Bania, K., Katsifis, D., & Circiumaru, A. (2022). *The Regulation of Cloud Computing: Getting It Right*. Available at SSRN 4285731., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4285731 [8 June 2026].

57 Ennis, S. / Evans. B. (2024): *Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence*; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4395183 [8 June 2026].

- Manganelli and Schnurr (2024): *Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies*[58]

Schnurr, D. (2022)

- Schnurr points out that while it is intuitively clear at a general level which cloud services belong to the different service types, this distinction is considerably more complex at a detailed level.
- Above all, distinguishing on the basis of the main objective and the underlying data processing model does not appear to be particularly helpful for establishing classification.
- Relevant text passage (underlining added):

  "The DA states that most of the rules on switching between data processing services (see Art. 23) as well as the functional equivalence test for IaaS services should only apply in the context of a customer switching to a service of the same service type. The concept of a service type is defined by Art. (2) (13) of the DA as "a set of data processing services that share the same primary objective and basic data processing service model". Although, on a broad level, it is to some extent intuitive what services belong to different service types (e.g., "data storage service" vs. "computing service" at the IaaS layer or "office suite" vs "enterprise resource planning software" at the SaaS layer), such a distinction becomes much more intricate on a granular level . For example, is a SaaS-based office suite that includes a video conferencing tool of the same service type as a stand-alone messaging and video conferencing service? Does a data analytics service belong to a different service type if it uses a different statistical approach than another analytics service? Here, the service type definition of the DA, which refers to the "primary objective" and the "basic data processing service model" of a service is not very helpful to resolve these questions and addressing the need for establishing a wider classification of service types for all data processing services. Given the large variety of data processing services that can also be highly differentiated between service providers, this introduces significant uncertainty about whether and when a data processing service will fall within the scope of the respective obligations of the DA."

Geradin et. al. (2022)

- Geradin et al. describe the definition of the term "service type" as problematic as it does not reflect the complexity of the value chain.

58 Manganelli, A., & Schnurr, D. (2024). *Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies*. Available at SSRN 5811422; retrievable at: https://cerre.eu/wp-content/uploads/2024/02/CERREreportCloudcomputingfeb24.pdf [8 June 2026].

- They point out that the definition of the same service type fails to take into account the fact that cloud services have certain features in common with competing offers but can differ significantly in terms of their provisioning for customers.
- Relevant text (underlining added):

  "However, in the context of cloud computing, the definition of "service type" is problematic because it does not reflect the complexity of the value chain, that is, the different service types (or service models) identified in Part II above. What is more, this definition does not consider that different cloud services of the same model may share certain features with competing offerings, but vary significantly in terms of how they are delivered to customers. This means that complying with obligations established in the DA, such as those imposed by Article 23(1) and Article 29(1), may be unfeasible in practice."

Ennis / Evans (2023)

- Ennis / Evans see the functional "same service type" classification as a legal construct that does not reflect reality; the same function can be achieved in different ways technically. Even if it is possible to determine a theoretical equivalence between functions, a given function is likely to be differently implemented by different cloud computing service providers and these differences ultimately reflect the fact that "developers have a different understanding of the needs of the same customers". This can render a switch under retention of "the same function" very expensive or impossible from a technical perspective.
- They additionally note that restricting the criterion of functional equivalence to the IaaS level is difficult and artificial as it is becoming more and more difficult in reality to distinguish between IaaS and PaaS levels.
- The authors therefore conclude that:
  - "service type" and "same service type" are legal concepts that are divorced from the technical realities of the cloud sector. The sector is characterised by a high degree of service innovations driven by the changing needs and requirements of customers.
  - "same service type" and "service type" in their defined form are only suitable as initial filters for capturing broad service families with which cloud customers are able to identify.
  - a far more detailed approach is necessary that should ultimately reflect the ability of cloud customers to differentiate.
  - the same service type should not be limited to the same service model.
- They therefore fear that this ambiguity could result in legal disputes that inevitably impede and even prevent the switching process.
- Relevant text (underlining added):

It is apparent that 'service type' and 'equivalent service' are legal concepts divorced from the technical realities of the cloud industry, which is characterised by high levels of service innovation driven by the changing needs and demands of customers. We find that 'equivalent service' and 'service type', as defined, are fit only to serve as an initial filter to capture broad families of services with which cloud customers may identify. Beyond 'equivalent service' and 'service type', a far more granular approach is necessary and should ultimately be reflective of the level of discernment exhibited by cloud customers.

The question has already been posed by others as to whether data analytics services that employ different statistical approaches should be considered as the same 'service type', or 'equivalent services'. In this case, to answer in the affirmative would lead to the absurd application of a legal finding of equivalence to technically heterogenous cloud computing services. We would underscore the concern that even where notional equivalence between functionalities may be identified, any given functionality is likely to be implemented divergently by different cloud computing service providers and that, critically, such divergence is reflective of the reality that "developers understand differently the needs of the same customers".

We would also note that equivalence should not be restricted to the same data processing service model, given the aforementioned problems inherent in the prevailing service model taxonomy. Although in this regard the definition contained in the Council text represents a minor advancement, it should be regarded that recital 71a regresses to the position that "[t]ypically, services falling under the same service type also share the same data processing service model."

It is inherently concerning that so much of the attempted reduction in ambiguity is situated in the increasingly dense thicket of recitals. Indeed, despite certain improvements, we fear that a pervasive absence of clarity could give rise to legal disputes that will necessarily complicate and even forestall the switching process. Moreover, the Parliament text appears to confirm that the functional equivalence criterion should apply only to the IaaS layer in the context of both portability and interoperability. In light of the earlier discussion of cloud service models, this exposes a profound disconnect between the legislator's understanding and the realities of the industry. We would underscore the reality that distinguishing between the IaaS and PaaS layers, in particular, is an increasingly challenging and artificial pursuit.

Manganelli / Schnurr (2024)

- Manganelli / Schnurr recommend that regulatory measures should take into account the specific economic and technical features of the cloud computing sector and the strategic decision-making processes of cloud customers.
- They note that recital 81 evidently implies that the term "same service type" could be closely connected with the concept of substitutability on the demand side.
- They also ascertain the following with regard to switching:
  - "…*in a specific situation, unbundling a particular service from the overall service supplied by the original DPS provider and moving it to another provider can also be considered as switching (recital* 85)."
  - Recital 93 actually states that *"…providers of data processing services should also be required to remove obstacles to unbundling a specific individual service from other data processing services provided under a contract and make the relevant service available for switching, in the absence of major and demonstrated technical obstacles that prevent such unbundling".*
  - This provision is difficult to decipher overall. It is in all probability to be interpreted in such a way that it only applies to the obligation to provide two services as independent services.

Manganelli and Schnurr (2024) also take into account the three countries that pursue an active approach with regard to the monitoring and regulation of cloud services: France (Autorité de la Concurrence), the Netherlands (ACM) and the United Kingdom (Ofcom). However, among the relevant publications of these three countries, only ACM's proposal of changes to the Data Act contains remarks on the concept of "same service type".

- The French National Competition Authority (NCA) notes in its comment[59] that "with regard to the Data Act… it makes sense to keep an eye on various aspects as the European Commission is to carry out an assessment of the legal provisions in three years, including … the establishment of measures for promoting data portability and interoperability".
- The British regulatory authority Ofcom published a market study on competition aspects on the cloud market in 2023.[60] Section 5 describes the obstacles for switching to a multi-cloud solution as well as technical restrictions and exit fees. There are no specific remarks concerning the concept of "same service type".

59 See Autorité de la concurrence (2023): *Avis n° 23-A-05 du 20 avril 2023 concernant le projet de loi visant à sécuriser et réguler l'espace numérique*; retrievable at https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2023-05/23a05.pdf [9 June 2026].

60 See OFCOM (2023): *Cloud Services Market Study*; retrievable at: https://www.ofcom.org.uk/internet-based-services/cloud-services/cloud-services-market-study [8 June 2026].

- In the Netherlands, the ACM published a final document on the investigation of the cloud market[61] and a proposal for improving the Data Act[62] in September 2022. The proposal envisages changes to the Data Act but distinguishes clearly between data portability and interoperability. However, it advocates removing the restriction of the obligations to same service types so that they apply to all service types.
- Furthermore, the ACM wishes to prescribe that
  - APIs are publicly accessible to facilitate interoperability.
  - egress fees are reduced not only in the case of portability, but also in the case of interoperability.
  - third-party providers are allowed to combine their services with the services of another cloud provider of the same quality offered within a given cloud.

Conclusion

The conclusion drawn from the analysed publications is that Geradin et al. (2022), Schnurr (2022) and Ennis and Evans (2023) all conclude that the fundamental service model (IaaS, PaaS, SaaS) is not conducive to classification (either because the distinction between IaaS and PaaS is problematic or because the services and the resulting value creation are differentiated to varying degrees). Ennis and Evans (2023) therefore conclude that determination of the same service type should not be limited to the same service model.

Schnurr additionally concludes that using the primary objective as a criterion is problematic because the distinctions between highly differentiated services become more complex as the granularity of the taxonomy increases. The specific requirement in the Data Act of functional equivalence for IaaS services (and therefore the portability and interoperability requirements) must also be viewed critically in this connection.

One suggestion standing out from approaches from other countries is that made by the Dutch ACM in 2022 proposing to completely remove the limit to same service type for data portability and interoperability.

3.2.1.2 General cloud taxonomies

Regardless of any reference to the Data Act, there are numerous general taxonomy approaches for cloud services in the literature. A distinction can be drawn in particular between technical and functional taxonomies. As a functional definition of “same service type” primarily underlies the Data Act (see section 3.1), the functional taxonomies are

61 See ACM (2022): *Market Study Cloud Services*; retrievable at „https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf [8 June 2026].

62 See ACM (2022): *Proposal to enhance the draft Data Act*, retrievable at https://www.acm.nl/system/files/documents/proposal-to-enhance-the-draft-data-act.pdf [8 June 2026].

particularly of interest in the present case. One of the first functional taxonomy approaches originates from *Armbrust et al. (2009)*. Their paper *Above the Clouds: A Berkeley View on Cloud Computing*[63] already distinguishes between compute, storage and networking as functional core competencies. Further taxonomies were developed on this basis in the following years, some of them considerably more refined (see, for example, *Höfer / Karagiannis (2011)*[64]; *Sikeridis et al. (2017)*[65]).

Above all the taxonomy approach of Sikeridis et al. (2017)[66] appears particularly worthy of attention with regard to the identification of services of the same service type in accordance with the Data Act as different service classes are formed (computing, storage, databases, analytics, data pipeline; machine learning; networking) to highlight similarities, common design approaches and functional differences. This at least comes close to a determination of the "same service type" in accordance with the Data Act, albeit that the service model level receives no attention from Sikeridis. The cloud market has likewise undergone very dynamic further development since the publication of this taxonomy, which means that the classification may appear somewhat obsolete from today's perspective at least in parts.

Khomchak (2024)[67] offers a more up-to-date taxonomy of cloud services in his comprehensive classification of the existing cloud services of the world's largest cloud providers, thereby producing a broad structural overview of the cloud services on the market. As well as 'classical' services (compute, storage etc.), Khomchak also includes modern areas here such as AI, quantum computing, VR / AR and blockchain. Khomchak distinguishes in this manner between 24 key cloud service features. This does not make the wording of Khomchak's taxonomy fully compatible with the Data Act as the key cloud service features represent a mixture of objectives and functions within the meaning of the Data Act. Nevertheless, with his comprehensive categorisation of the existing cloud services of the largest providers, Khomchak provides valuable insights for the classification model to be established in this study, especially with regard to the range of services to be covered by the classification model.

Sikeridis et al. (2017):

63 Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing (Vol. 17). *Technical Report UCB/EECS-2009-28*, EECS Department, University of California, Berkeley. Retrievable at: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/Archive/EECS-2009-28.pdf.

64 Höfer, C. N., & Karagiannis, G. (2011). Cloud Computing Services: Taxonomy and Comparison. *Journal of Internet Services and Applications*, 2(2), 81-94.

65 Sikeridis, D., Papapanagiotou, I., Rimal, B. P., & Devetsikiotis, M. (2017). *A Comparative Taxonomy and Survey of Public Cloud Infrastructure Vendors*. arXiv preprint arXiv:1710.01476. See https://www.researchgate.net/publication/320223370; retrievable at: https://arxiv.org/abs/1710.01476 [8 June 2026].

66 See footnote 66.

67 Khomchak, M. (2024). A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection. *International Journal of Computing*, 23(3), 468-475., retrievable at: https://computingonline.net/files/journals/1/archieve/IJC_2024_23_3_17.pdf [08.06.2026].

- Comparative functional taxonomy for public cloud infrastructures
- Systematisation:
  - **Compute**
    - Virtual machines (VMs)
    - Container services
    - Serverless / Function as a Service (FaaS)
    - High-performance computing (HPC)
  - **Storage**
    - Object storage
    - Block storage
    - File storage
    - Cold / archival storage
  - **Databases**
    - Relational databases
    - NoSQL databases
    - In-memory databases
    - Managed database services
  - **Analytics**
    - Data warehousing
    - Big data processing
    - Real-time analytics
    - Data lakes
  - **Data pipelines**
    - ETL services
    - Streaming services
    - Message queues
    - Data integration services
  - **Machine learning**
    - Training platforms
    - Managed ML frameworks
    - AI APIs
    - Model deployment services
  - **Networking**
    - Virtual private cloud (VPC)
    - Load balancing
    - Firewalls & security groups
    - Content delivery networks (CDN)

Khomchak (2024)

- Broad-based, functional and market-oriented public cloud service taxonomy

with 24 main categories (key cloud service features)
- Compute
- Storage
- Databases
- Networking
- Developer tools
- Analytics & big data
- AI/ML
- Security & identity
- IoT
- Migration & hybrid cloud
- Management & governance
- Mobile services
- Enterprise integration
- End user computing
- Front-end web & mobile
- Business applications
- Blockchain
- Gaming
- Multimedia services
- Content delivery networks
- Satellite services
- Robotics
- Quantum computing
- VR / AR

3.2.1.3 Norms and standards with regard to cloud systems and service model

A review was initially carried out of the standards, definitions and norms published with regard to service models for cloud services, such as NIST and ISO/IEC. This was followed by an investigation of whether there were other relevant publications regarding service models to be taken into account, as the service model is part of the definition of the concept of "same service type".

The first definition of cloud service models dates back to the "**Cloud Computing Reference Architecture**" published by NIST in 2011.[68]

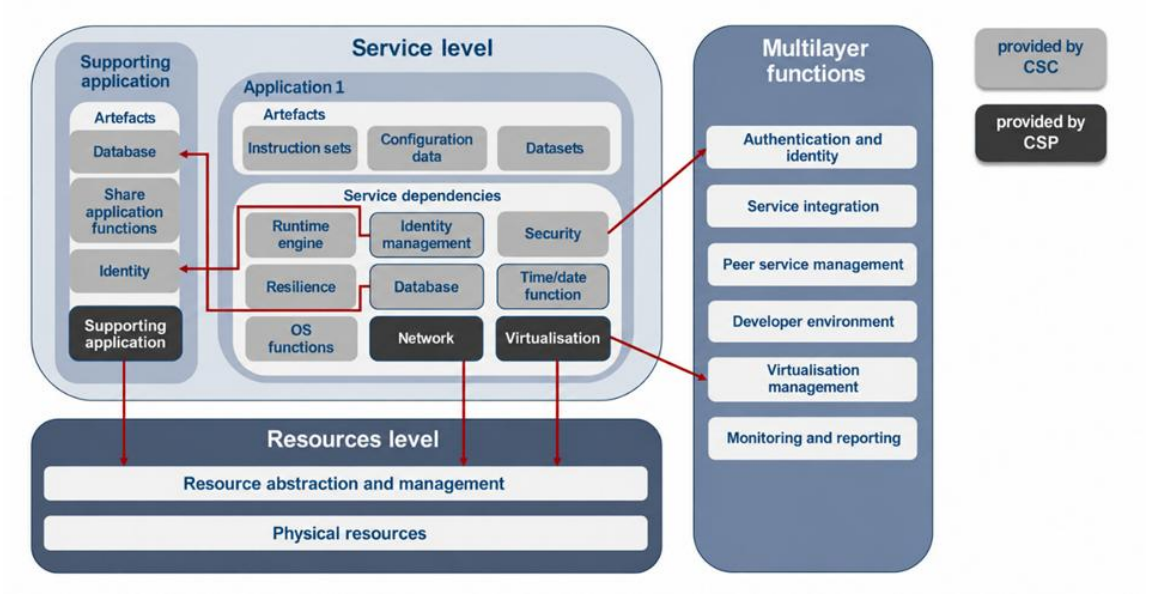
68 NIST SP 800-145 "The NIST Definition of Cloud Computing" (2011). See https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf.

- NIST describes the three service models SaaS, PaaS and IaaS that provide "…*consumers with different types of service management operations and expose different entry points into the cloud system…"*
- A distinction is drawn between the cloud provisioning models public, private and community cloud.
- The definitions of IaaS / PaaS / SaaS, in Appendix A, point 13-15, are as follows (underlining added):
    - ***Software as a Service (SaaS)****: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client NIST SP 500-292 NIST Cloud Computing Reference Architecture 21 devices through a thin client interface such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings*.
    - ***Platform as a Service (PaaS)****: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations*.
    - ***Infrastructure as a Service (IaaS)****: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).*

ISO/IEC 19941[69] then followed in 2017 with a focus on data portability and interoperability, with the various service models describing which components are provided either by the cloud service customer (CSC) or the cloud service provider (CSP). This standard is set to be replaced by ISO/IEC DIS 19941-1 in the months to come. The figures below illustrate the differences between IaaS, PaaS and SaaS graphically.

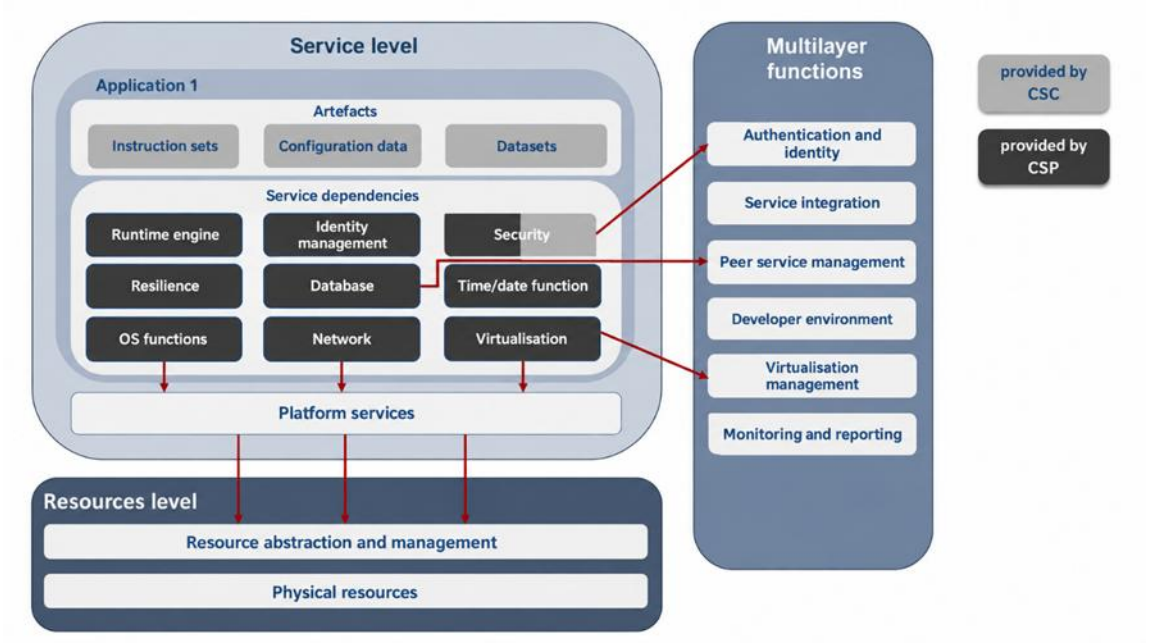
69 See https://www.iso.org/standard/87817.html.

Figure 3-2: Illustration of an application run in an IaaS environment



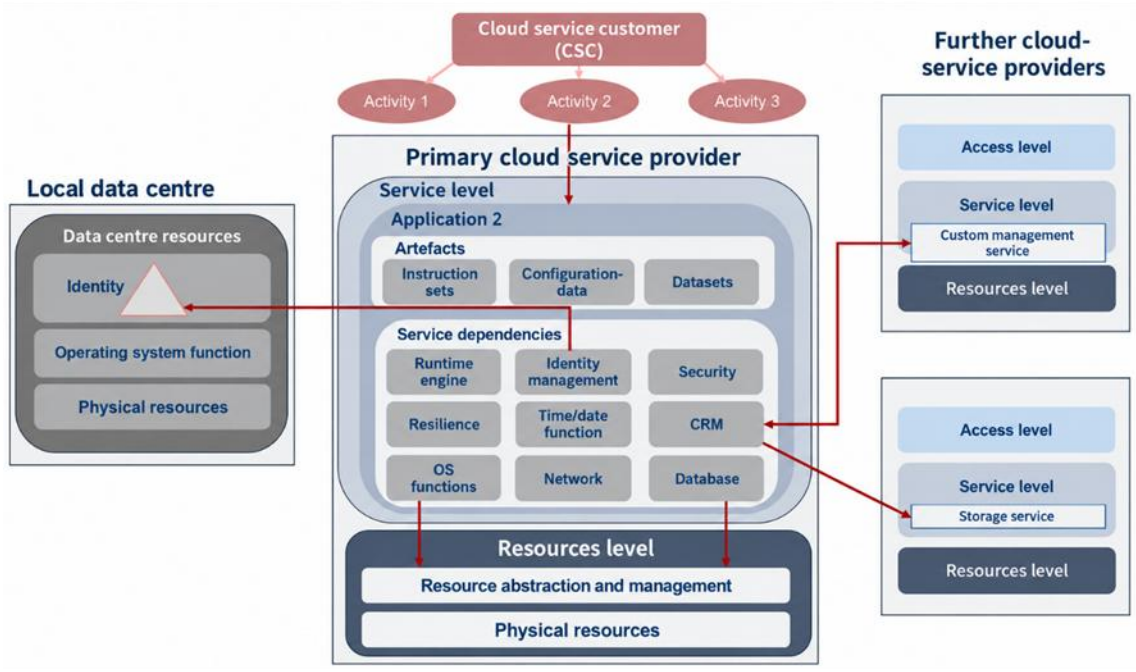
Source: ISO/IEC 19941:2017 – Figure 14. Own configuration by WIK-Consult.

Figure 3-3: Illustration of an application run in an PaaS environment



Source: ISO(IEC 19941:2017 – Figure 15. Own configuration by WIK-Consult.

Figure 3-4: Illustration of an application run in an SaaS environment



Source: ISO(IEC 19941:2017 – Figure 17. Own configuration by WIK-Consult

Another relevant publication regarding the service model topic is Noor et al (2020).[70] The publication examined detailed properties and new cloud functions to facilitate an enhanced comparison of service models. The following new categories were added:

- Financial Software as a Service
- Education as a Service
- Business Process as a Service
- Gaming as a Service
- Health Informatics as a Service
- Software Engineering as a Service
- Security as a Service
- (Edge) Analytics as a Service
- Cloud as a Service

70 Noor et al (2020):, H., Malik, B. H., Khatoon, M., Ali, H. W., & Nasim, R. (2020). Brief Comparison Of Cloud's Emerging Services: A Literature Review. *International Journal of Scientific & Technology Research*, 9.

This was followed in 2023 by **ISO/IEC 22123-1, -2 and -3[71]:** This norm provides a consolidated terminology for cloud services and their capabilities. It replaces ISO/IEC 17788:2014.

- The norm provides a classification of cloud services in line with the cloud capabilities type. It distinguishes between the following types:
  - Application capabilities type: the customer of the cloud service can use the applications of the cloud service provider;
  - Platform capabilities type: execution environments are provided to the customer of the cloud service by the provider in which applications created or acquired by the customer can be executed and managed.
  - Infrastructure capabilities type: computing, storage or network resources are provided to the customer of the cloud service.
- In addition, specific "as a service" models were defined that are assigned to the various types. As well as the familiar models IaaS, PaaS and SaaS, these also include the following "as a service" models:
  - Communication as a Service (CaaS) – both application capabilities and platform capabilities
  - Compute as a Service (CompaaS) – infrastructure capabilities
  - Data storage as a Service (DSaaS) – can be provided in all three types
  - Network as a Service (NaaS) – can be provided in all three types

ISO/IEC TS 7339:2024[72] followed in 2024: "Information technology – Cloud computing – Overview of platform capabilities type and platform as a service". In view of the inclusion of technologies such as AI and quantum computing in more traditional service concepts, the authors consider it expedient to distinguish between the PaaS concept intended for a specific purpose and the more general type of "platform functions". This separation is carried out at the main functionality level through the separation of digital functions.

Conclusion

ISO/IEC 19941:2017 is currently the most up-to-date norm in which the service models are described in detail. However, it is soon to be replaced by ISO/IEC DIS 19941-1. The most up-to-date definitions of terminology are contained in ISO/IEC 22123-1-3, published

71 ISO/IEC 22123-1:2023. Information Technology – Cloud Computing. Part 1: Vocabulary (Edition 2, 2023). ISO/IEC 22123-2:2023. Information Technology – Cloud Computing. Part 2: Concepts. ISO/IEC 22123-3:2023. Information Technology – Cloud Computing. Part 3: Reference Architecture (Edition 1, 2023); the norms can be retrieved here: [8 June 2026].

72 ISO/IEC TS 7339:2024 - Information technology - Cloud computing - Overview of platform capabilities type and platform as a service.

in 2023. An important aspect of this is the assignment of different “as a service” models that can be used for classifying the service types:

- Communication as a Service (CaaS) → application or platform
- Compute as a Service → infrastructure
- Data Storage /Network as a Service → infrastructure, application or platform

These additional service models differ from the aaS models proposed by Noor (2020). The focus of Noor lies either on the applications (Financial aaS, Education aaS, Gaming aaS, Health Informatics aaS, Analytics aaS, Security aaS) or on a platform (Business Process aaS, Software Engineering aaS, Security aaS, Cloud aaS).

3.2.2 Proposed main objectives of data processing services

Because there are no new suggestions in the literature regarding the main objectives, the following draws on the main objectives already identified in section 3.1.1.:

1. The processing of data (**PD**);
2. The storage and retrieval of data (**SRD**);
3. The transmission of data (**TD**);
4. Making available digital functions (**DF**).

The next step consists of identifying the possible main functionalities and assigning them to the defined main objectives. It will then become clear whether the selected main objectives sufficiently cover all functionalities.

3.2.3 Proposed main functionalities of data processing services

The categories of functionality identified in the literature review were drawn on for defining the main functionalities in the classification model. Functional categories of the commercial cloud services currently on offer were additionally taken into account.

The list drawn up of potential main functionalities was subsequently cleansed of all product or market segment labels. The result is shown in the table below in the “Sub-functionalities” column.

A review was conducted in the next step of whether certain functional categories can be pooled. The following criteria were applied for this:

- Distinction between “main functionalities” (can be offered independently) and “sub-functionalities” (can only be offered in combination with the main functionality).

- If multiple main functionalities are identified, the one at the centre determines the (subjective) allocation.
- “Functional equivalence” within a main functionality and thus within a group of cloud services with the same service type must be ensured.

Functional equivalence exists if the same main functionalities are provided by different data processing services of the same service type, regardless of their technical implementation (see also section 3.1).

Functional equivalence does **not** mean that two services must be identical. Different providers can implement the same functionality via different technical architectures or technologies. For example, a database service can be functionally equivalent even if:

- different database engines are used,
- the internal architecture is designed differently.

The decisive factor is that the customer is able to achieve the same functional purpose with the service.

This resulted in the table below. As well as the available service model and the main objective, the customary functional classification in the market is described (functionalities/generic sub-functionality). The final column shows the main functionality used for classification into same service types, with the aforementioned criteria (offered independently, at the centre and functional equivalence) duly taken into account.

Table 3-1: Initial step towards taxonomy

Available service models	Main objective	Functionality	Generic sub-functionality	Main functionality applied (for same service types)
IaaS	PD	Compute	Virtual infrastructure	Virtual machine hosting
IaaS	PD	Compute	Virtual infrastructure	Bare metal
IaaS	PD	Compute	Virtual infrastructure	Batch & HPC
PaaS	PD	Compute	Managed orchestration	Container orchestration
PaaS	PD	Compute	Managed orchestration	Serverless containers
PaaS	PD	Compute	Managed orchestration	Function as a Service (FaaS)
PaaS	PD	Compute	Specialised compute	Quantum processors
PaaS	PD	Compute	Specialised compute	Quantum algorithms
PaaS	PD	Compute	Specialised compute	Quantum solver
PaaS	SRD	Storage	Standardised data stores	Object storage
IaaS	SRD	Storage	Standardised data stores	Block storage
PaaS	SRD	Storage	Standardised data stores	File systems
PaaS	SRD	Storage	Data protection & archive	Archive storage
PaaS	SRD	Storage	Data protection & archive	Backup & disaster recovery
IaaS/PaaS	TD	Connectivity	Core transport	Dedicated interconnect
IaaS/PaaS	TD	Connectivity	Core transport	Virtual private network (VPN)
IaaS/PaaS	TD	Connectivity	Core transport	Network security / VPC
PaaS	DF	Web & edge	Content delivery	Content delivery network (CDN)
PaaS	DF	Web & edge	Content delivery	Content distribution

Available service models	Main objective	Functionality	Generic sub-functionality	Main functionality applied (for same service types)
PaaS	DF	Web & edge	Content delivery	Edge caching
PaaS	DF	Web & edge	Content delivery	Load balancing
PaaS	DF	Data platforms	Database engines	Relational databases
PaaS	DF	Data platforms	Database engines	NoSQL databases
PaaS	DF	Data platforms	Database engines	In-memory databases
PaaS	DF	Data platforms	Analytics & big data	Data warehouse
PaaS	DF	Data platforms	Analytics & big data	Data lakes
PaaS	DF	Data platforms	Analytics & big data	Stream processing
PaaS	DF	AI & ML	Intelligence services	Computer vision
PaaS	DF	AI & ML	Intelligence services	Speech-to-text
PaaS	DF	AI & ML	Intelligence services	Natural language AI
PaaS	DF	AI & ML	Intelligence services	Machine learning lifecycle
PaaS	DF	App integration	Messaging & API mgmt	Enterprise messaging
PaaS	DF	App integration	Messaging & API mgmt	API management
PaaS	DF	App integration	Messaging & API mgmt	Workflow orchestration
SaaS	DF	Productivity	Managed collaboration	Managed communication (email/chat)
SaaS	DF	Productivity	Managed collaboration	Collaboration & productivity tools
IaaS/PaaS/SaaS	DF	Productivity	Managed collaboration	Desktop as a Service (VDI)
SaaS	DF	Ent. apps	Standardised business logic	CRM
SaaS	DF	Ent. apps	Standardised business logic	ERP/SCM
SaaS	DF	Ent. apps	Standardised business logic	HCM
SaaS	DF	Ent. apps	Standardised business logic	ESG & carbon tracking
SaaS/PaaS	DF	Operations	Mgmt & governance	Identity and access management (IAM)
SaaS/PaaS	DF	Operations	Mgmt & governance	Data protection
SaaS/PaaS	DF	Operations	Mgmt & governance	Cost management / FinOps
PaaS	DF	Development	Dev. ecosystem	CI/CD
PaaS	DF	Development	Dev. ecosystem	Code hosting

Source: WIK-Consult / Decision

The next step comprised an examination of which sub-functionalities can be aggregated to capture the service type appropriately and practically for later implementation. This is intended to prevent the scope of “switching requirements” from being restricted and/or cloud providers from “positioning” their services in different service types compared to their competitors so that the switching requirements do not apply.

3.2.4 Identification of the service models of data processing services

Section 3.1.2 explained that the service model represented the same type of service provision, that is, how the service is technically provisioned, used, managed and invoiced. This concerns the resources and functionalities made available.

The Data Act distinguishes between the following service models for the provision of data processing services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and other services offered “as a Service” (XaaS).

The service model (IaaS, PaaS or SaaS) can be identified on the basis of ISO/IEC 19941 or its successor ISO/IEC DIS 19941-1. ISO/IEC 22123-1 to 3 can be used for the

assignment of new types of aaS model to one of the traditional service models. The provision of Noor (2020) can be used for service models not described (eg Finance as a Service) to place the focus either on an application (SaaS) or on a general platform (PaaS).

As the switching requirements in the Data Act are tied to the same service type (including service model), no formal requirements apply to cloud providers if a customer switches to another service model for a comparable functionality.

If specific main functionalities are only provided in a given service model, the distinction “same service type” based on the service model is practically non-existent. However, there are cloud services that provide specific main functionalities in different service models (IaaS, PaaS, SaaS depending on the provider).

Examples are:

- Virtual desktop (Windows 365): is offered as an SaaS service by Microsoft; however, competitor Azure offers VDI as a PaaS service and other cloud providers offer VDI as part of their IaaS services.
- Containers are offered in both the IaaS and PaaS model or monitoring and registration tools such as AWS Graphene (offered in PaaS) but which are offered by other cloud providers in the SaaS model.

It is customary on the market for customers to switch upwards in the technology stack (from IaaS to PaaS and from PaaS to SaaS), but sometimes also downwards (back to PaaS and IaaS). Reasons for this can be high costs and/or the decision to switch back to on-premise solutions.

In view of this market reality and the fact that the Data Act also addresses hybrid cloud solutions including local infrastructure, it does not seem appropriate for it to limit the switching requirements to functionally equivalent cloud services with the same provisioning model.

3.2.5 Proposed classification

The actual classification model is ultimately derived from the preceding analyses and discussions and is illustrated below in Table 3-2.

The classification model is intended to facilitate an initial classification of the individual configurations to be examined by the supervisory authority. An in-depth consideration is then to be carried out on this basis taking account of all relevant circumstances.

The essential combination for the “same service type” is derived from the columns in light blue. The columns to the right of this (levels 0 to 2) describe the customary functional

classification in the market. This serves here to facilitate a simpler assignment of cloud services. In addition to this classification, examples of customary services in the market and a description of the technical delimitation criteria have been added.[73]

The classification model constitutes the essential output of section 3 by pooling all previous considerations and analyses in this section.

Owing to the core significance of the classification model (Table 3-2) for this section and the further course of the study, Table 3-3 provides interpretation and usage instructions for the classification model.

73 Please note: as long as a service has not yet developed fully on the market, a more general category is usually appropriate. If, however, the services are already further developed and consolidated, more specific subcategories are often possible.

Table 3-2: Proposed classification model

Service model	Main objective	Main functionality	Level 0	Level 1	Level 2	Specification of delimitation/portability (What makes the main functionality unique?)	Example
IaaS	PD	Virtual infrastructure	Compute	Virtual infrastructure	Virtual machine hosting	Virtual CPU/RAM/OS interface	EC2 / Azure VMs / Compute Engine
			Compute	Virtual infrastructure	Bare metal	Physical hardware interface	EC2 bare metal / bare metal instances / bare metal solution
			Compute	Virtual infrastructure	Batch & high performance computing (HPC)	Job/scheduler API	AWS Batch / Azure Batch
PaaS	PD	Managed orchestration	Compute	Managed orchestration	Container orchestration	Kubernetes API / Manifest	AKS, EKS, GKE + for web apps, full delegated services such as Azure App Service, AWS Elastic Beanstalk
			Compute	Managed orchestration	Serverless containers	Container resource spec	AWS Fargate, Google Cloud Run, Azure Container Apps
			Compute	Managed orchestration	Function as a Service (FaaS)	Function code and / or runtime API	Cloud functions such as Lambda
PaaS	PD	Specialised compute	Compute	Specialised compute	Quantum processors	Quantum circuit interface	Braket / Azure Quantum
			Compute	Specialised compute	Quantum algorithms	Algorithm which is specific to quantum computing	Braket SDK / Q#
			Compute	Specialised compute	Quantum solver	Functional output schema	Braket Solvers / Q-Solvers
PaaS	SRD	Standardised data stores	Storage	Standardised data stores	Object storage	S3 REST API	Azure Blob Storage, AWS S3, object storage at GCP / OVH / Scaleway
IaaS			Storage	Standardised data stores	Block storage	Volume interface	EBS, Managed Disks, Persistent Disks
PaaS			Storage	Standardised data stores	File systems	Common Internet File System (CIFS) & Server Message Blocks (SMB) protocols	Azure Files, FSX
PaaS	SRD	Data protection & archive	Storage	Data protection & archive	Archive storage	Retrieval functionalities (incl. cold storage specific APIs)	Glacier, Archive Tier
			Storage	Data protection & archive	Backup & disaster recovery	Data recovery point objective (RPO)	AWS Backup, Azure Backup, Cloud Backup
IaaS/PaaS	TD	Dedicated interconnect	Connectivity	Core transport	Dedicated interconnect	L2 physical port	Direct Connect, ExpressRoute, Cloud Interconnect, Direct Link
IaaS/PaaS	TD	Virtual private network (VPN)	Connectivity	Core transport	Virtual private network (VPN)	L3 IPsec tunnel	VPN Gateway
IaaS/PaaS	TD	Network security / VPC	Connectivity	Core transport	Network security / virtual private cloud (VPC)	Classless Inter-Domain Routing (CIDR) & security rule schema	VPC, VNET
PaaS	DF	Content delivery	Web & edge	Content delivery	Content delivery network (CDN)	Cache policy logic	CloudFront, Front Door
			Web & edge	Content delivery	Content distribution	Data replication scheme	CloudFront, Front Door
			Web & edge	Content delivery	Edge caching	Edge runtime API	Lambda@Edge, Edge functions
			Web & edge	Content delivery	Load balancing	Routing rules, service health checks (incl. load balancing algorithm)	ALB, NLB, Traffic Manager
PaaS	DF	Relational databases	Data platforms	Database engines	Relational databases	SQL / database schema	Azure SQL, RDS, Cloud SQL
PaaS	DF	NoSQL databases	Data platforms	Database engines	NoSQL databases	Data model / query API	Dynamo DB, Cosmos DB, Firestore, Managed NoSQL

Service model	Main objective	Main functionality	Level 0	Level 1	Level 2	Specification of delimitation/portability (What makes the main functionality unique?)	Example
PaaS	DF	In-memory databases	Data platforms	Database engines	In-memory databases	Throughput settings + key / value API	ElastiCache, Redis, Memory Store
PaaS	DF	Data warehouse	Data platforms	Analytics & big data	Data warehouse	SQL / database schema	RedShift, Synapse, BigQuery
PaaS	DF	Data lakes	Data platforms	Analytics & big data	Data lakes	File format (Parquet) & Catalog API	Hadoop, Microsoft Fabric One Lake
PaaS	DF	Stream processing	Data platforms	Analytics & big data	Stream processing	Windowing & event logic	Kinesis, Stream, Analytics Dataflow, Managed Apache Flink
PaaS	DF	Intelligence services	AI & ML	Intelligence services	Computer vision	Image-in / metadata-out	Rekognition / AI Vision / Vertex Vision
			AI & ML	Intelligence services	Speech to text	Audio-in / transcription-out	Transcribe / speech / speech to text
			AI & ML	Intelligence services	Natural language AI	Text-in / sentiment analysis-out	Comprehend / language / natural language ==> Current market covered by LLMs
			AI & ML	Intelligence services	Machine learning lifecycle	Model format (open neural network exchange)	SageMaker / Azure ML / Vertex AI
PaaS	DF	Enterprise messaging	App integration	Messaging & API mgmt	Enterprise messaging	Message schema / queue lifecycle policy	SQS & SNS / service bus / pub/sub / managed queues
PaaS	DF	API management	App integration	Messaging & API mgmt	API management	Open API specification (may also include authorisation policy)	API Gateway / APIM / Apigee
PaaS	DF	Workflow orchestration	App integration	Messaging & API mgmt	Workflow orchestration	State machine definition	Step Functions / Logic Apps / Workflows
SaaS	DF	Managed collaboration	Productivity	Managed collaboration	Managed communication (email/chat)	User profile & protocol (IMAP)	OVH Mail, M365 Exchange / Teams, Google Chat, GMail
SaaS	DF		Productivity	Managed collaboration	Collaboration & productivity tools	Document formats & permissions	Managed Nextcloud, SharePoint, Monday.com...
IaaS/PaaS/SaaS	DF	Desktop as a Service (VDI)	Productivity	Managed collaboration	Desktop as a Service (VDI)	Display protocol (Terminal Services / Remote Desktop Protocol (RDP))	Windows 365, AVD
IaaS/SaaS	DF	CRM	Ent. apps	Standardised business logic	Customer relationship management (CRM)	Parameterised customer data fields + workflows	Salesforce / Dynamics 365 / Salesforce
IaaS/SaaS	DF	ERP/SCM	Ent. apps	Standardised business logic	Enterprise resource planning (ERP) / supply chain management (SCM)	Parameterised data fields + workflows	SAP / Dynamics 365
IaaS/SaaS	DF	HCM	Ent. apps	Standardised business logic	Human capital management (HCM)	Parameterised HR fields + workflows	Workday / Dynamics 365
SaaS	DF	ESG & carbon tracking	Ent. apps	Standardised business logic	ESG & carbon tracking	Reporting schema (eg carbon emissions per annum)	
SaaS/PaaS	DF	Mgmt & governance	Operations	Mgmt & governance	Identity and access management (IAM)	Security Assertion Markup Language (SAML) / OpenID Connect (OIDC)	Entra ID, Google IDP, Okta, Active Directory, ADFS
			Operations	Mgmt & governance	Data protection	Key management policy (configuration file)	KMS, Key Vault
			Operations	Mgmt & governance	Cost management / FinOps	Billing API & resource tagging	CloudHealth, Cost Explorer, cloud billing APIs
PaaS	DF	Dev. ecosystem	Development	Dev. ecosystem	Continuous integration (CI) / continuous delivery (CD)	Pipeline definition (configuration file)	CodePipeline, Azure DevOps
			Development	Dev. ecosystem	Code hosting	Git interface	Azure DevOps, Github, Code Commit

Source: WIK Consult / Decision

Table 3-3: Illustration of the interpretation of the classification model based on an excerpt from the model

Service model	Main objective	Main functionality	Level 0	Level 1	Level 2	Specification of delimitation/portability (What makes the main functionality unique?)	Example
IaaS	PD	Virtual infrastructure	Compute	Virtual infrastructure	Virtual machine hosting	Virtual CPU/RAM/OS interface	EC2 / Azure VMs / Compute Engine
			Compute	Virtual infrastructure	Bare metal	Physical hardware interface	EC2 bare metal / bare metal instances / bare metal solution
			Compute	Virtual infrastructure	Batch & HPC	Job/scheduler API	AWS Batch / Azure Batch
PaaS	PD	Managed orchestration	Compute	Managed orchestration	Container orchestration	Kubernetes API / Manifest	AKS, EKS, GKE + for web apps, full delegated services such as Azure App Service, AWS Elastic Beanstalk
			Compute	Managed orchestration	Serverless containers	Container resource spec	AWS Fargate, Google Cloud Run, Azure Container Apps
			Compute	Managed orchestration	Function as a Service (FaaS)	Function code and / or runtime API	Cloud functions such as Lambda
PaaS	PD	Specialised compute	Compute	Specialised compute	Quantum processors	Quantum circuit interface	Braket / Azure Quantum
			Compute	Specialised compute	Quantum algorithms	Algorithm which is specific to quantum computing	Braket SDK / Q#
			Compute	Specialised compute	Quantum solver	Functional output schema	Braket Solvers / Q-Solvers
PaaS	SRD	Standardised data stores	Storage	Standardised data stores	Object storage	S3 REST API	Azure Blob Storage, AWS S3, object storage at GCP / OVH / Scaleway
IaaS			Storage	Standardised data stores	Block storage	Volume interface	EBS, managed disks, persistent disks
PaaS			Storage	Standardised data stores	File systems	CIFS & SMB protocols	Azure Files, FSX
PaaS	SRD	Data protection & archive	Storage	Data protection & archive	Archive storage	Retrieval functionalities (incl. cold storage specific APIs)	Glacier, Archive Tier
			Storage	Data protection & archive	Backup & disaster recovery	Data RPO	AWS Backup, Azure Backup, Cloud Backup
IaaS/PaaS	TD	Dedicated interconnect	Connectivity	Core transport	Dedicated interconnect	L2 physical port	Direct Connect, ExpressRoute, Cloud Interconnect, Direct Link
IaaS/PaaS	TD	Virtual private network (VPN)	Connectivity	Core transport	Virtual private network (VPN)	L3 IPSec tunnel	VPN Gateway
IaaS/PaaS	TD	Network security / VPC	Connectivity	Core transport	Network security / VPC	CIDR & security rule schema	VPC, VNET



Data Act – the combination defines “same service type”	Features of data processing services in order to determine the service type it falls under.	Delimitation criteria: check whether the data processing service really does fall under the same “main functionality”	Evaluation: if the same technical interface is used (see previous column), the switch from one service to another is technically feasible and reasonable.

Source: own illustration (WIK / Decision)

3.3 Analysis of modular / partial switch of services

The following section examines the requirements for a customer to request a modular switch when changing provider.

3.3.1 Definition of a “modular switch”

A partial or modular switch relates to the scenario in which a customer redeploys one or more specific data processing services to another provider while continuing to use other services of the original provider.

The term “modular switch” does not thereby constitute an autonomous legal concept of the Data Act but describes a group of switching cases in which the customer does not replace the entire service package of a provider, but merely migrates individual services, service components or functional layers. From the customer perspective, the possible exercise of the rights granted by the Data Act when switching data processing services depends in this case on whether such a partial migration is covered by the right to switch defined by the Data Act. The strongest legal starting point for modular switches is embodied by Article 23 of the Data Act, which explicitly mentions the simultaneous use of multiple providers and the separation of a provider’s data processing services to the extent that this is technically possible. Article 23 of the Data Act argues that contractually bundled data processing services may not be withheld from isolated switching solely on account of their packaging. If a component can be identified as a data processing service in its own right and there are no significant and proven technical obstacles, the bundling of multiple services to form a package can pose a contractual or organisational impediment to switching that must be removed. Such an impediment contradicts the purpose of Chapter VI of the Data Act of facilitating effective switching, multi-provider use, portability and interoperability and reducing lock-in effects. The “same service type” requirement must only be taken into account for modular switches if the switch is assessed as a switch to another data processing service of the same service type. It must furthermore be borne in mind that the same service type requirement applies neither to switches to the customer’s on-premises ICT infrastructure nor to the simultaneous use of multiple providers. A modular switch in other constellations can therefore also come into question in these cases. This is actually less problematic legally as long as the same service type restriction is lifted.

The facilitation of modular switches creates the flexibility to ensure that customers are not forced into an “everything or nothing” migration but can instead select the “best-of-breed” service based on comparable functionality and efficiency. This partial switch can take different forms:

- Unbundling of commercial offers: this concerns services bundled by the CSP but sold individually as stand-alone software packages;

- Unbundling across models: this concerns the “extraction” of the technical layers (IaaS, PaaS, SaaS) of the services to be switched. Application can take place within the same service type or across different service types (eg unbundling is conceivable for the VDI or SharePoint bundle of services; see also section 3.3.5);
- Functional unbundling: this concerns cloud services grouping multiple main functionalities (as defined in our assessment framework). These can be unbundled to enable the customer to switch a specific functionality.

3.3.2 Different scenarios for unbundling

The unbundling approach must take account of the different technical and commercial configurations in which data processing services are used. The primary approach consists of removing specific services from a larger environment to ensure that migration still remains technically feasible if services are provided as part of a complex stack or commercial package. We distinguish four main scenarios that determine how services are decoupled for a partial switch:

- Unbundling of a commercial package: services are not procured individually but as part of a predefined commercial package (eg a security suite or productivity package). The approach consists of viewing each service as a group of functional modules. A customer must be able to unbundle a specific module and migrate it to a target provider while the other services of the original package continue to be operated on the initial infrastructure.
- Services offered within the same provisioning model: this scenario comprises the unbundling of services that are operated at the same technical level of the cloud stack (eg PaaS-to-PaaS). For instance, a customer may wish to switch its managed ETL pipeline to a specialised provider while keeping its managed database analytical service on the same initial platform. As both services are at the same level, the focus of unbundling is on the logical separation of dataflows and management interfaces.
- Services that are provided via different provisioning models: A modular switch frequently takes place vertically across provisioning models. A typical example would be the unbundling of an SaaS business application (eg SharePoint in our previous examples) from the underlying virtual IaaS infrastructure. This approach requires the source provider to facilitate extraction of the superordinate digital assets (in our SharePoint example this would correspond to the files and folder structure and the role-based access controls associated with the files) while the stability of the infrastructure level remains guaranteed if the customer decides to remain there.
- Functional unbundling within a service: In cases in which an individual cloud service contains multiple main functionalities (as defined in our classification), it

must be possible for these to be unbundled if they represent independent functional objectives. As these functionalities are provided within a single technical product, they are offered by definition in the same provisioning model. If, for instance, a uniform data platform provides both data storage and workflow orchestration, the customer must be able to switch the orchestration functionality independently.

3.3.3 Five-step approach to the analysis of modular switching

An approach is presented in the following section for the practical analysis of modular switching. It can be divided into five steps:

Step 1: Stocktaking

Stocktaking roughly comprises entry of the initial service data and the removal of 'marketing' reference points to leave a functional service description (what the service does, not who sells it or what brand it is). A review of whether a data processing service as defined in the Data Act actually exists also falls under this step (see assessment framework in section 2).

Step 2: Targeting

Traditional boundaries between infrastructure components can become blurred in the modern cloud landscape as highly integrated services can cover multiple functional areas. This impedes classification for the supervisory authorities: many services, such as managed databases, AI platforms or intelligent content delivery networks, can operate simultaneously across the four identified main objectives (processing, storage, transmission and digital functionalities). If no longer suffices to rely on a purely descriptive list of technical features as this leads to overlapping definitions and creates loopholes that CSPs can exploit to classify their services incorrectly and circumvent strict switching requirements associated with the same service types.

In order to establish a viable taxonomy, the approach must go beyond the question "What can the service do?" and instead concentrate on the primary intention of the service, ie the dominant functionality representing the core value proposition for which the customer pays. By separating the primary functionality from the other capabilities, we aim to ensure that even the most complex hybrid service is assigned to a single primary objective.

- **Measure: assign each service to one of the four main objectives:**
  - **PD (processing**): does the service execute code? (computing power/AI)
  - **SRD (storage**): does the service permanently store data? (hard drives/archives)

- **TD (transmission**): does the service transmit raw data between endpoints? (VPN/connection)
- **DF (digital functions**): does the service provide a preconfigured logic or application results? (SaaS/PaaS)

The main reason for carrying out this review is to ensure that hybrid services are tied to a single main objective to prevent CSPs from 'concealing' advanced services in simpler and less regulated categories.

Step 3: Generic functional clustering (the "buckets")

The services are grouped in stage 3 according to the 27 main functionalities set out in the assessment framework.

This gives rise to a benchmark for determining the "same service type" and prevents cloud providers from objecting to a customer's request to switch on the grounds that switching is not possible because the specific "sub-sub-functionality" is lacking in the target cloud. If a module falls in the "relational database" category, its main functionality is comparable with every other service in this category, regardless of its proprietary sub-functionalities.

Step 4: Assessment of the technical limits and interfaces

This is equivalent to the assessment of the "specification of delimitation/portability" as set out in the assessment framework. For IaaS this is normally operating system management, for PaaS the API or the language (eg SQL) and for SaaS rules and datasets.

Step 5: Grey zone and avoidance of overlaps

Proposal of a generic methodology for managing future grey zones

In a fully differentiated cloud market, grey zones are not the result of unclear definitions but a direct consequence of technical convergence. As the cloud architectures develop further, the boundaries between infrastructure, platform and software logic are becoming blurred. An individual technical asset can now simultaneously cover multiple functional areas. For example, a network tool might also guarantee application security or a storage system execute data life cycle logic. This fuzziness causes complexity within the classification criteria (main objective, main functionality and service model). If these criteria appear to be in conflict with each other, a grey zone arises that permits multiple valid technical interpretations of the same service.

It is important for a supervisory authority to identify and describe these grey zones. Cloud providers could use these grey zones to circumvent requirements (eg by classifying an intelligent transmission network as mere data transport). It is possible by documenting

these overlaps and providing a mandatory regulation for risk reduction for each individual grey zone to ensure that the switching requirements of the Data Act are also applied consistently to these grey zones.

In order to counteract the complexities related to cloud convergence described above, it is proposed that a number of logical tests be applied that are designed to remove functional overlaps. This approach aims to prevent “grey zones” from being used as regulatory loopholes.

A regulatory authority could apply the following four criteria:

- Evaluation of namespace and API: it is necessary first to assess whether two services use a shared logical account and namespace and a shared management interface. If “archives“ and “standard” use the same S3-compatible API and bucket namespace, this comprises the same service type from a technical perspective, regardless of marketing-based service levels.
- Evaluation of the logical endpoint: the OSI layer at which the processing provided by the provider ends must be determined. If a service assesses or processes data at layer 7 (application layer) or forwards data to such level, its functionality is deemed to transcend mere data transport. It must therefore be classified as a digital function. This fundamentally applies to services active above OSI layer 4.
- Evaluation of the primary objective and settlement: the “final state” paid for by the customer pays is determined. If settlement is dependent on the success of a retrieval and not on data persistence, the service is tied to a digital function objective, with storage treated as a secondary component.
- Evaluation of the functional performance: the internal model architecture is ignored specifically for AI and generative AI and the focus should be on the achieved business task. If two models, a specialised and a general one, both generate translated text, they are functionally equivalent for the purpose of the switch.

3.3.4 Unbundling of individual cloud services offered via different provisioning models

In this scenario, individual cloud services are offered in different provisioning models but bundled commercially. For example, virtual machines (VMs) provisioned as part of IaaS for operation of the customer database are combined with an analysis platform provisioned as part of PaaS. Now the customer wishes to switch the VM to another provider or another analysis platform.

As the Data Act obliges cloud providers to remove all commercial obstacles, we will concentrate here on the technical aspects while nevertheless pointing out that

commercial obstacles could by all means exist (such as a non-existent combination of products a customer would like to have).

We illustrate the approach by means of an example of the unbundling of IaaS / PaaS / SaaS:

> One of the greatest obstacles to modular provider switching is the bundling for which cloud providers use different provisioning models (IaaS, PaaS, SaaS and XaaS) in order to claim that the services comprise different "types" that are therefore not comparable. Supervisory authorities should look beyond these descriptions to identify the functional objective of the service and, wherever possible, classify components of the service package as digital assets. The functional purpose thus constitutes the final result or situation the customer wishes to achieve with the service, regardless of the technical architecture used for provisioning. The functional purpose is more detailed than the generic main functionalities in the assessment framework.
>
> A good example of this challenge is virtual desktop infrastructure (VDI). Microsoft sells Windows 365 as an SaaS product and offers a "Cloud PC" with fixed prices and a fully managed control level. By contrast, Azure Virtual Desktop (AVD) is a PaaS/IaaS hybrid where the customer is responsible for management of the images of virtual machines, the scaling logic and infrastructure orchestration. Despite these different management levels, the functional main objective for the user remains identical: the provisioning of a remote desktop environment.
>
> In order to facilitate a modular switch in this scenario, the supervisory authority could prescribe that the user profile and personalisation data be treated as digital assets. Regardless of whether a profile is loaded onto a simplified SaaS instance (Windows 365) or a highly customisable PaaS cluster (AVD), the underlying data processing service remains the same type. This way it would be possible to counter the argument of the cloud providers that the SaaS character of a product renders it incomparable with a PaaS-based alternative.
>
> This principle is even more meaningful if one is moving outside the "sphere" of an individual provider, for instance if a customer wishes to switch from a highly automated SaaS environment such as Windows 365 to another cloud service provider such as OVHcloud VDI or Scaleway Elastic Metal. Such a switch should be possible without the customer losing the digital assets they have built up over the years. For example, the export of user profiles via standardised, non-proprietary tools such as FSLogix could be prescribed, thereby safeguarding the **continuity of the functional purpose** for the customer. This would prevent technical "stratification" from being used as an instrument for vendor lock-ins.

3.3.5 Application of the methodology to real use cases and grey zones

Grey zones typically arise if the following classification criteria conflict with each other:

- main objective versus technical implementation
- main functionality versus service model
- input type versus functional output

Below we provide examples by way of illustration with suggestions for remedy:

Object storage

- On the one hand the service can be broadly defined: object storage is a primary memory (for storing live data).
- On the other hand, object storage is also used for backup and archiving functions (there are other main functionalities in the classification model that cover this).

We propose carrying out risk reduction as follows:

- The following must be noted with regard to backups:[74] the technical delimitation of a backup solution is usually easy to identify since a backup platform generally lies outside the service to avoid risks (damage, accidental deletion, cyber incidents). Versioning is an integrated feature of object storage technology and does not facilitate genuine data protection. The data and snapshots may be lost in the event of data corruption or accidental deletion as they are stored on the same technology platform. However, a backup replicates the data on another storage platform, thereby enhancing data stability. For the supervisory authority this prevents providers from claiming that the storage components are an infrastructure service that cannot be separated from the backup logic.

- The distinction between hot and archive storage is a further problem from the customer perspective; it appears to comprise the same service. The overlap is logical as “archive” is rarely a separate physical storage location but rather a status or “level” of the same object. However, cloud providers prefer to classify hot and archive storage as different services to justify different price and access architectures. To shape this distinction efficiently, the “namespace principle” can be applied: if the data are in the same bucket and retrieved through the same API, they relate to the same service type. It could furthermore be argued that the export of “tiering metadata” potentially be prescribed. This ensures that when moving their data, customers not only switch the bits but also the cost-saving “cold” or

74 Except for bucket versioning as this does not comprise genuine backups but an integrated feature of the platform.

"hot" status of these data and thus replicate the same financial structure with the new provider. However, implementation is very complex.

Consolidation of the AI market:

The AI sector is currently undergoing massive consolidation that is creating a significant grey zone. We distinguish separately in our classification between image processing, voice recognition and natural language; modern "foundation models" and generative AI platforms now cover almost all these categories via a single interface. This poses the risk of a provider claiming that its generic service is unique and not comparable with an older service (eg ChatGPT versus Nano Banana, one of the Gemini modules).

While this is a complicated case, our suggestion for risk reduction consists of drawing on the "functional output" again instead of the "input type" (image vs. text). If two services offer the same service, eg image recognition, they have a comparable main functionality regardless of its implementation (specialised versus broad model). In this particular case the main functionality could be fine-tuned at a later stage to "intelligent output" instead of to subcategories based on the input such as computer vision, voice or AI vision.

Advanced network services:

There is a further grey zone regarding the distinction between pure data transfer (transfer of bits via standard data transport technology) and intelligent data transfer (transfer of bits including logic). This grey zone results from the fact that network hardware is becoming increasingly software-defined. For example, a global load balancer looks like a network tool but fulfils functions at the application level such as SSL termination and request routing. Cloud providers frequently conceal these under network functions to argue that they are merely pure transport functions. The suggestion for remedying this problem is to examine how the logical termination of the service is structured; if the service verifies or caches the data, this constitutes a digital function (DF) and not just transport (TD). This serves to ensure that the complex routing and caching rules of the user that confer additional intelligence to the standard network are protected when switching.[75]

Identity vs. security status (posture) management:

One could consider whether there are overlaps between identity and access management (IAM) and security status management. It is not possible in modern network implementations (branded "zero trust") to separate "Who has access?" (identity) from "Is the resource safe?" (security status). Furthermore, both services frequently make use of the same dashboards and policy engines. To reduce this grey zone, it is suggested that the "security policy" be viewed as a portable digital asset. A switch is then only compliant if the security configurations (the JSON or YAML files that define the security posture)

75 Illustration: AWS Direct Connect provides the data transfer connection (data transfer), while AWS CloudFront assumes the caching and routing logic (content delivery).

can be transmitted and applied to the new environment, thereby preventing any reduction in the customer's security baseline during the migration.[76]

3.3.6 Results of the interviews

This section presents the key findings from a total of 10 expert interviews conducted between April and May 2026 with suitable corporate representatives of international and European cloud providers and German cloud customers. The interviews were conducted as online meetings in sessions lasting approximately 45 minutes.

Care was taken to ensure that on the supplier side both the world's largest cloud providers and leading European providers were represented. Attention was paid on the customer side to ensuring that both large companies and SMEs were canvassed through the interviewees. For reasons of confidentiality, the results of the interviews are pooled in the presentations below to prevent any conclusions from being drawn about specific companies. General assessments by the interviewees concerning Chapter VI of the Data Act are addressed initially (section 3.3.6.1), before the focus is placed subsequently on the modular switch (section 3.3.6.2).

3.3.6.1 Overall assessment and classification of Chapter VI of the Data Act by the interviewees

Profound scepticism concerning the practical relevance and feasibility of the Data Act was manifested across all interviews. The reasons for this attitude can be subdivided into different categories:

Conceptional and definitional comments

The vagueness and perceived limited practicability of the configuration of core terms and concepts of the Data Act were frequently mentioned in the interviews.

For instance, the **concept of "same service type"** is viewed critically. Globally leading and other providers argue that a static taxonomy of service types is not practical as the market is developing too dynamically. Both large and smaller cloud customers also reported that this concept had not so far been an issue at their companies. This points to a significant lack of transparency on the customer side concerning the new provisions for cloud switching.

The **concept of functional equivalence** is also viewed critically by leading global providers. They warn that an obligation to guarantee "functional equivalence" during a

76 Illustration: Microsoft Entra ID manages the users as Microsoft Defender for Cloud verifies the resources that these users access. A modular substitution would require the portability of the underlying security policies that connect them both.

switching procedure could in effect serve to enforce a “synchronisation” of services. This could stifle innovation and restrict the choices available to customers.[77]

In addition, some providers question whether the **SaaS level** really ought to fall within the scope of application of the Data Act. One SaaS provider from the B2B sector also argues that many of the services they offer strictly speaking do not fall under the definition of Article 2(8) of the Data Act and therefore do not constitute data processing services within the meaning of the Data Act. This is used to support the hypothesis that the Data Act was originally designed primarily for the IaaS level. The underlying regulatory logic of the IaaS level could not simply be transferred to the SaaS level. The providers point out that the switching of B2B SaaS solutions can take several years due to necessary reconfigurations and renewed customer-specific adjustments. With this in mind they call for the SaaS level to be excluded from the scope of application of Chapter VI of the Data Act.

A switch at the PaaS level is frequently described as considerably more complex and challenging than a switch at the IaaS level. Many providers often associate it in their argumentation with the difficulties of the SaaS level.

The following reasons are cited for this:

- Unlike IaaS, which is based on standardised “components”, significant architectural differences frequently lie behind PaaS services (such as “Database as a Service” and SQL instances). A switch here not only involves the exporting of data but also the adjustment of entity structures, query dialects (SQL dialects) and specific function calls
- Switching from IaaS to PaaS entails an increased use of provider-specific functionalities and integrated features. This results in greater dependence on the provider’s respective ecosystem and makes the switch considerably more complex than an IaaS-to-IaaS switch.

The same state of affairs is described for cross-layer switching: switches between different layers (eg from PaaS to IaaS) are possible but entail a major technical outlay due to widely varying APIs and data formats. A “downward migration” (SaaS to PaaS/IaaS) is rare, while customers are more likely to migrate “upwards” in order to outsource complexity to the cloud providers.

Obstacles to the effectiveness of the Data Act

The provisions of the Data Act for switching provider are described particularly by large customers as not effective as the largest global providers generally worked with high

77 It is not possible to draw any conclusions at this stage concerning the customer perspective on the concept of functional equivalence as this issue did not form part of the structured questionnaire used for discussions with customers.

discounts and long-term contracts. Furthermore, customers were provided with “innovation budgets” by the major cloud providers if the latter had the impression that the customer might be willing to switch. The effects emanating from the Data Act for facilitating a switch of provider tended to fizzle out in the face of such discounts and “innovation budgets”. Furthermore, large customers report that they rely in any case on multi-cloud strategies and generally make parallel use of the services of all the largest global providers. These customers accordingly also do not expect any significant impact of the Data Act on provider switching.

A further obstacle to effectiveness particularly in the eyes of smaller providers is the fact that egress costs would only be removed gradually and not immediately. This would perpetuate the dominant position of the largest providers. The smaller providers therefore favour the immediate and complete abolition of egress costs.

Cloud customers also point out that they consider it a mistake that the Data Act first and foremost governs one-off switching (ie with “switch-off” at the existing provider) and the continuous exchange of data between different providers within the scope of multi-cloud strategies does not receive the same attention. Customers would welcome it here, for example, if a provision were to exist stipulating that when exchanging data the egress costs must be equivalent to the ingress costs as this is the same procedure from a technical perspective and the different pricing cannot be justified with corporate outlay.

It became clear from the talks with medium-sized customers that the lack of knowledge about the specific configuration of the regulation concerning provider switching also posed a significant obstacle to the effectiveness of the Data Act. The opportunities offered by the regulation are frequently not seen here, with smaller companies in particular often also lacking the technical know-how to classify the significance of the regulation for their own business. One medium-sized customer suggested expanding the transparency and communication obligations of cloud providers towards customers to draw attention to changed underlying conditions and switching rights. Public information and knowledge transfer campaigns as support measures are also considered appropriate.

Concerns regarding European competitiveness

European providers in particular pointed out in the discussions that the Data Act had been continuously watered down in the various negotiation rounds so that the objective of creating a joint level playing field with the major providers could no longer be achieved through the Data Act in its current form.

One European provider is also bringing a “Buy European” approach into play for public and private institutions. The largest providers were already too big to be beaten in the free market.

Large customers also do not see any major chances of success with the current regulatory approach of the Data Act with regard to strengthening the competitive position of European providers. Massive investments in the European cloud infrastructure are considered more promising. The world's largest cloud providers were significantly more competitive at present, meaning that switching to a European provider was not even possible for certain applications / services, even if the customer were to wish to do so. This aspect was underlined particularly by large customers. "Convenience" aspects play an important role from the perspective of smaller companies: it was simply more convenient / easier to use the services of the largest international providers (such as Office 365), particularly against the backdrop of a lack of resources (time, money, know-how). For this reason, many did not actively consider cloud-switching scenarios and consequently also did not make use of potential rights arising from the Data Act from the customer perspective. Here too the effects of the Data Act with regard to provider switching were seen to fizzle out.

3.3.6.2 Views and opinions about modular switching

Modular switching at the IaaS layer from the provider perspective

The providers see IaaS services as "modular combinable components" that are designed by their nature to be unbundled and combined independently from each other. From a technical perspective, modular switches at the IaaS level therefore rarely pose problems. The European providers welcome the rules at the IaaS level concerning full and partial provider switching as a means of mitigating lock-in effects among the world's largest providers. However, one European provider criticises the failure of the Data Act to set out any clear and binding standardisation roadmap. The largest global providers could therefore play for time as a result of this, meaning that modular switching at the IaaS level may for the time being remain more costly and thus perpetuate lock-in effects.

Modular switching at the SaaS layer from the provider perspective

The providers' assessment at the SaaS layer fundamentally differs to that at the IaaS level: there is broad consensus among large and smaller providers that unbundling at the SaaS level is "not practical" or "extremely difficult". One of the largest global providers compares the replacement of individual components within a fully integrated SaaS solution with the attempt to replace components of an Airbus aircraft with Boeing components while expecting them to function smoothly.

Modular switching at the PaaS layer from the provider perspective

Modular switching at the PaaS layer is also frequently described as considerably more complex and challenging than at the IaaS level. The argumentation is similar to that relating to the SaaS layer. PaaS is considered a kind of "grey zone" in which modular

switching is theoretically conceivable but in many cases disproportionately expensive or a technical risk due to provider-specific adjustments and deep integration.

Customer perspective and modular switching

Customers report considerable economic obstacles to modular switching. Some corporate customer contracts contain provisions stipulating a massive price increase for the services remaining with the original provider following a partial or modular switch. As a result, customers frequently allow services to run on that they actually no longer need simply to avoid the price increase for the rest of the package. This consequently reduces the practical relevance of modular switching in practice, with many customers instead opting for parallel operation. This logic applies particularly to larger customers receiving high “all-in-one” discounts.

Large corporate customers also point out that volume-based contracts with minimum purchase guarantees can limit the practical relevance of a partial switch: if by switching one were to fall below the minimum purchase guarantees, this would lead to rising costs as there would be no cost savings with the existing provider but additional costs would be incurred from the new provider.

At the same time, large customers also mention that the modular use of services of different providers is very widespread within the scope of multi-cloud strategies. However, this is not so much a case of one-time modular switching, but more of the modular structuring of the company’s cloud environment. For instance, one large cloud customer mentions that the company relies particularly on an LLM model of a large provider that is then integrated into other services of other providers wherever the use of LLMs is called for.

The topic of “modular switching” has so far barely attracted any attention if at all from the medium-sized customers interviewed. Owing to the limited resources, this topic is already too specialised and complex to be addressed upfront in the company. The view here is that the issue could be encountered reactively, that is, if the company were to be dissatisfied with an existing provider and therefore to address in detail the options for switching. However, this has so far not been the case among the medium-sized companies interviewed. The issue is not being addressed proactively.

Technical perspective of customers / providers concerning modular switching

Large customers stress that open APIs and interoperability for data exchange are crucial for partial switching. However, this applies not only to switches, but also to the continuous exchange of data between services.

Nevertheless, some providers warn that the mandatory prescription of standardised APIs could restrict innovation owing to a “synchronisation” of services.

The providers also underline the possibility of technical restrictions such as latency and performance requirements in some cases, meaning that services would have to remain at the same data centre or on specific hardware. This could in effect prevent a partial migration to another provider in these cases.

Although not primarily a purely technical argument but more a question of governance, a further aspect put forward by managed service providers (MSPs) in particular is that resources located in the environments of other providers could no longer be managed by the MSP, rendering an unbundling of such managed cloud services on the basis of the business model impossible.

3.3.6.3 Conclusion on the findings from the interviews

Overall, the interviews show that the practical effect of Chapter VI of the Data Act with the intended reduction of lock-in effects and associated facilitation of provider switching is viewed sceptically: core concepts such as “same service type” appear to many market participants to be too unclear, static or technically difficult to operationalise; at the same time, long-term contracts, discount structures, “innovation budgets”, minimum purchase obligations and the initial continuation of egress costs serve to weaken the intended interplay. This is further exacerbated from the customer perspective by the fact that smaller and medium-sized users in particular are frequently unaware of their new rights or do not make use of them strategically for lack of resources and technical expertise.

Modular switches are considered technically realistic above all at the IaaS level, while at the SaaS level they are predominantly found to be barely practical owing to strong integration and customer-specific adjustments. From the customer perspective, discount models, minimum purchases and price increases following partial cancellations serve to significantly reduce the practical appeal of such switches. It is therefore not so much selective modular switching that dominates in practice as the parallel use of multiple providers within the scope of multi-cloud strategies. Core requirements remain open APIs and interoperability, although standardisation obligations are simultaneously considered in some cases to be a potential obstacle to innovation.

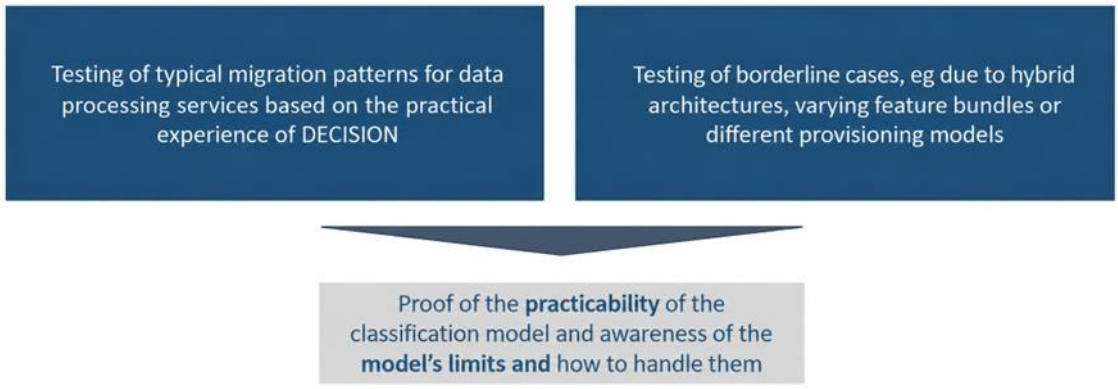
While the normative objective of Chapter VI finds broad understanding among those interviewed, its effectiveness is considered to be limited by a lack of conceptual clarity, economic counter-incentives, technical complexity and the structural strength of the largest global providers. As well as a clearer standardisation roadmap and improved information obligations, above all substantial investments in high-performance European cloud infrastructures are therefore considered decisive for strengthening European digital sovereignty.

3.4 Testing of the developed classification model

The previously developed classification model was tested in several stages:

- First the technical delimitations per service type were defined.
- Following the identification of grey zones (ambiguities within a defined service type) the technical delineation was further specified to eliminate those ambiguities.
- Based on the proposed classification, automatic assignment of the cloud services offered in the EU was carried out. Non-assignable services were assessed to establish whether there was another reason for their non-assignment (test services, migration tools).

Figure 3-5: Overview of the testing of the model



Source: WIK-Consult

All categories were reviewed to determine whether there were specific subcategories that potentially overlap or trigger ambiguities. Where this was found to be the case, an examination was carried out first of all to determine whether an additional technical delimitation could remove the ambiguity. If this was not the case, other solutions were sought for, such as the creation of a new category.

- A potential problem was identified for the category “specialised functions” (quantum processing, algorithms, solvers) as these could be highly specialised due to their XXL size (up to 2,468 TB). A new category “Quantum” was added to solve the problem.

The transition from definitions to the practical enforcement of provisions requires an iterable logical framework. This section describes the operational workflow for applying the developed taxonomy to real cloud services. This process ensures that each service

can be precisely assigned to its core category, regardless of its commercial presentation or technical complexity. This takes place by way of a structured sequence of events, from identification of the granular service through to the final definition of delimitation.

The five-tier categorisation logic previously presented for modular switching (see section 3.3.3) is also applied here. By connecting each cloud service to a specific main functionality and a distinct service model, the categorisation logic eliminates the ambiguities frequently accompanying proprietary or vertically integrated cloud stacks. Care is taken in so doing to ensure that the delimitation of the services in our classification model is geared to upholding the customer's business continuity and not to the internal architecture of the provider.

The following table illustrates the review of the technical delimitation between combinations of main functionality and sub-functionality, for instance in line 2 of the table between HPC scheduler and its applicable main functionality (columns 1 and 2) on the one hand and quantum algorithm and its applicable main functionality (columns 3 and 4) on the other. The final column describes how the technical delimitation between the two combinations is to be reviewed.

Main functionality 1	Sub-functionality 1	Main functionality 2	Sub-functionality 2	Review of technical delimitation
Virtual infrastructure	HPC scheduler	Specialised compute	Quantum algorithms	Possible sources of confusion: • Both provide high-quality, complex processing for calculations. • Both are attributable to PD as the main objective. Boundary testing: The delimitation is clear. One service manages standard computing resources, while the other manages quantum states. The service types differ as an HPC job cannot be replaced by a quantum circuit without rewriting the entire mathematical model.
App integration	Enterprise messaging	Content delivery	Load balancing	Possible sources of confusion: • Both receive an incoming message and decide in a rule-based manner where to forward it to. • Both are attributable to DF as the main objective. Boundary testing: The delimitation of load balancing consists in the synchronous forwarding of requests to an active backend, for instance at HTTP or OSI Layer 7. If the backend is not available, the request backfires. By contrast, the delimitation of enterprise messaging is asynchronous: the service guarantees the buffering and/or queueing of messages. The message is kept available until a consumer is ready.

Main functionality 1	Sub-functionality 1	Main functionality 2	Sub-functionality 2	Review of technical delimitation
Data protection & archive	Archive storage	Analytics & big data	Data lake	Possible sources of confusion: • Both are designed to store petabytes of data at low cost for long periods. • Users frequently load data to both systems. Boundary testing: • The boundary for **active storage** is determined by SLAs for **availability** and **durability**. The input is a blob or comparable object; the same applies to the output. • By contrast, the boundary of a **data lake** is geared to **metadata** and **schema**. The input consists of raw data, while the output is a dataset that is integrated into an analytics catalogue. • A data lake can be retrieved to obtain a structured dataset. This is not the case with archive storage, where there are retrieval delays.
Managed collaboration	Desktop as a Service (VDI)	Virtual infrastructure	Virtual machine hosting	Possible sources of confusion: • Both provide a Windows or Linux environment. From a technical perspective, a user could use a virtual machine as a desktop environment. • DF vs. PD functionalities Boundary testing: VDI can be understood as a standardised service (SaaS/PaaS) because the user configures it via desktop parameters, while virtual machines constitute basic resources (IaaS). They do not belong to the same service type because the portability of the user profile is paramount when switching VDI, while the image portability is decisive when switching VM.
Standardised data stores	Block storage	Standardised data stores	Managed file systems	Possible sources of confusion: • Both provide storage resources. • Both are SRD. Boundary testing: • The boundary for block storage lies in the volume attachment and/or block I/O interface. Storage is attached to a single VM instance. • The boundary for managed file systems lies in the network protocol interface (NFS, SMB) and there is no 1:1 correlation between the storage and the consuming resource (simultaneous access).
Mgmt & governance	Identity & access management	Mgmt & governance	Data protection	Possible sources of confusion: • Both are security tools that permit or block access to data. • Both are DF. Boundary testing: • The boundary for IAM lies in the identity claims and/or role schema (SAML/OIDC). It defines who is a participant and which authorisations he has. • The boundary for data protection, for example in the case of a KMS, lies in the cryptographic key lifecycle and in the encryption policy. These define how the data are encrypted and who possesses the key to decode them again.

Main functionality 1	Sub-functionality 1	Main functionality 2	Sub-functionality 2	Review of technical delimitation
Core transport - basic	Network security / VPC	Content delivery - advanced	CDN	Possible sources of confusion: • Both services are responsible for transmitting data from a source to a destination. Boundary testing: • The objective of network security / VPC is the core transport that ensures that the package reaches its destination safely without reviewing the application content. • By contrast, a CDN has advanced functionalities and works at higher levels of the OSI model (above Layer 4). It reviews the package content and displays adaptive behaviour such as caching, load balancing etc. • When switching, the migration of a VPC is essentially a question of the migration of an IP address range or CIDR block, while a CDN relates more to the migration of behaviour rule sets.
Database engines	Relational database	Analytics & big data	Data warehouse	Possible sources of confusion: • Both are SQL databases. • Both store tables, columns and rows. • Both are retrieved via the open standard specification SQL (or variants derived from this). Boundary testing: • The boundary of a relational database is transaction integrity (ACID = atomicity, consistency, isolation and durability). The input consists of operations at row level. • By contrast, the boundary for a data warehouse lies with more aggregated data and analytical modelling requirements such as “calculate the average output of 10 million users”. It is optimised for massive, read-intensive analytical scans.

4 Market overview of data processing services

4.1 Identification of the key providers in the cloud market of the EU

4.1.1 Glance at the overall market

A market volume of almost **€177 billion** is forecast for the EU's **cloud market**[78] for **2026**. The EU thus has a share of the global market (€1.1 trillion) of just under **16%**. Germany represents the largest market within Europe and the third largest in the world with a volume just short of **€42 billion**. By far the largest market is the USA with a volume of **€508 billion**, followed by China with **€119 billion**.

The forecast annual **growth rate** for the global cloud market for the year 2026 amounts to 21.2% (EU: 20.45%). At around **17.17%**, the growth rate in Germany is significantly below the EU average. The volume of the EU market has almost quadrupled since 2020 (€45 billion). The market volume is expected to almost double again by 2030 (€320 billion). The cloud market therefore continues to post high growth rates, albeit that the growth is slowing compared with the previous years.

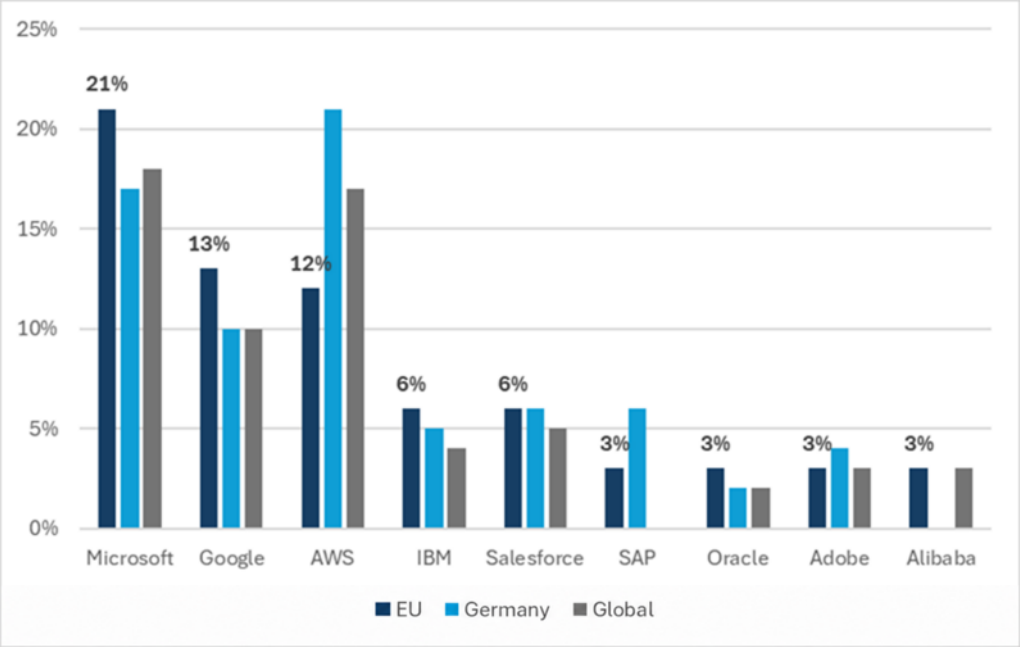
The largest providers on the **cloud market in the EU** are Microsoft (21%), Google Cloud (13%) and AWS (12%). These are followed by Salesforce and IBM with 6% each, after which come SAP, Oracle and Adobe with 3% each.

AWS is the leading provider in **Germany** with 21%, followed by Microsoft (17%), Google (10%) and SAP (6%). Salesforce likewise reaches 6% and IBM lies at 5%.

Compared with the European average, AWS therefore has a considerably stronger market position in Germany. The same applies to SAP as a German company. Here the share is double that of the European average. Globally SAP's share lies below 2% and is therefore not included in the statistics of the largest global providers (see Figure 4-1).

78 For the market data concerning the cloud market here and in the following (overall and separated into the IaaS, PaaS and SaaS markets), we draw on data from Statista: Statista. (2026). Public Cloud – Worldwide. Statista. https://www.statista.com/outlook/tmo/public-cloud/worldwide?currency=EUR. The latest available data have been drawn on (market volumes: June 2025; market shares: December 2023); last retrieved on 23 June 2026.

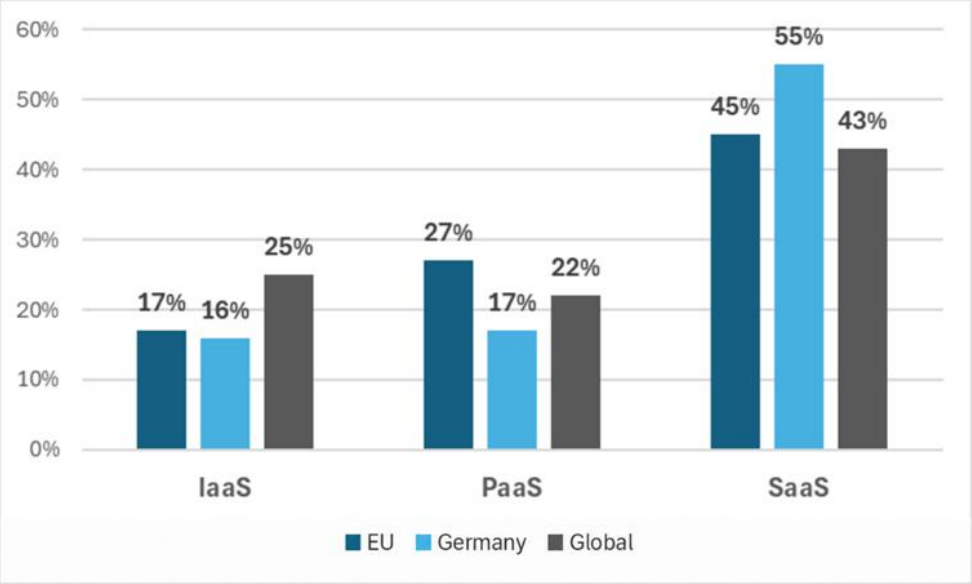
Figure 4-1: Market shares on the overall public cloud market



Source: own illustration; data: Statista (2026); where figures are missing: market share lies below 2%.

Below the overall market is split by service model (IaaS, PaaS, SaaS) and examined with regard to the key providers of data processing services in these submarkets. Figure 4-2 shows how the market shares are broken down across IaaS, PaaS and SaaS in the EU, in Germany and globally.

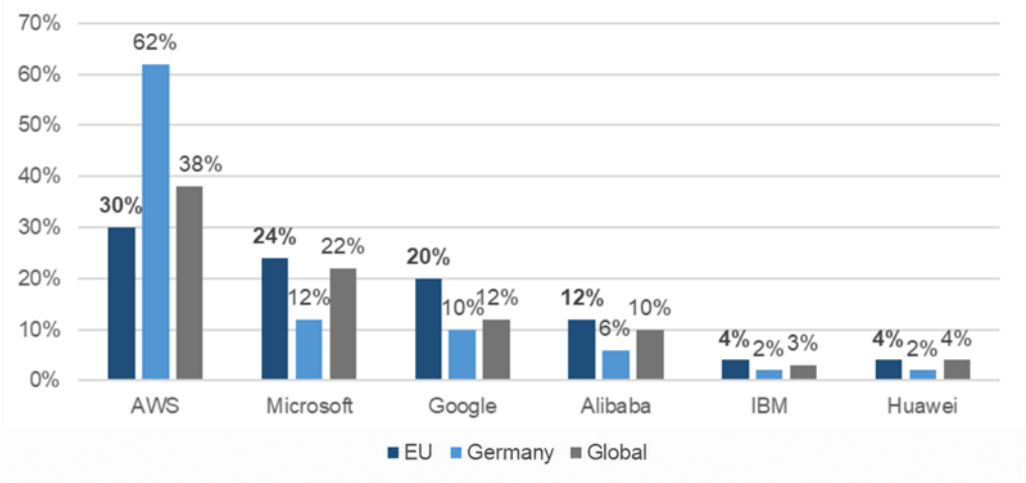
Figure 4-2: Breakdown of the market to the service models IaaS, PaaS and SaaS



Source: own illustration; data: Statista (2026), difference to 100% is split across other service models.

4.1.2 The IaaS market

Figure 4-3: Participants on the IaaS market



Source: own illustration; data source: Statista (2026)

The IaaS market has a volume of around €30 billion in the EU. This is equivalent to a share of 17% in the EU cloud market, which is below the 25% IaaS share in the global cloud market. The share in Germany amounts to 16% and is therefore close to the EU average (see Figure 4-2).

IaaS is currently one of the growth drivers in the cloud market (growth rate of 18.06% expected in the EU in 2026). This is attributable among other things to the rise in demand for computing capacities owing to the increased implementation of AI solutions. In addition, the topic of "sovereign cloud" in particular is a growth driver of IaaS.[79]

The IaaS market has a particularly high market concentration in comparison with other cloud segments. The top three providers in the EU have a market share of 74%: these are **AWS** (30%), **Microsoft** (24%) and **Google** (20%). The global share of the three companies lies at 72% (AWS: 38%, Microsoft: 22%, Google: 12%). The market in Germany is even more concentrated: 84% of the market volume is attributable to the top three, with AWS alone accounting for 62% (Microsoft: 12%; Google: 10%).

Further providers with relevant market shares include **Alibaba** (EU: 12%; global: 10%; Germany: 6%), **IBM** (EU: 4%; global: 3%; Germany: 2%) and **Huawei** (EU: 4%; global : 4%; Germany: 2%). All other providers have a market share below 2%.

79 See https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024.

The largest European provider in the IaaS segment is **OVHCloud** from France (total company revenue: approx. €1 billion). Its market share in the European IaaS market fluctuates between 1% and 2%.[80]

Another important player is the German provider **Hetzner**, which focuses on a clear price strategy for bandwidth-intensive workloads. As a result, Hetzner provides 3.79% of internet traffic in the EU, which is more than AWS (2.45%) and Google (1.71%). A reinforcing factor alongside the price strategy is also the desire of European customers for data sovereignty. Many customers of Hetzner are start-ups, medium-sized SaaS providers and SMEs.[81] Owing to its strategic focus, Hetzner's importance as outlined above is not reflected in its share of the market volume of the IaaS market (< 1%).

IONOS has become a specialist provider of IaaS solutions in particular for small and medium-sized companies on the European market and therefore plays an important role in the medium-sized business segment. This position is supported by its classification as a "major player" in the IDC market report [82] for IaaS providers in Europe despite its altogether moderate share of the overall market.

Deutsche Telekom with its IT subsidiary **T-Systems** is likewise classified by IDC as a "major player" in the European IaaS market. Its relevance is also based less on a dominant market share than on its deliberate strategic positioning in the field of sovereign, compliance-oriented cloud infrastructures. T-Systems particularly addresses regulated sectors such as healthcare and finance and the public sector with corresponding services.[83]

The following providers have therefore been identified as particularly relevant in the European IaaS market:

<u>The largest providers:</u>

- **Alibaba**
- **AWS**
- **Google**
- **Huawei**
- **IBM**
- **Microsoft**

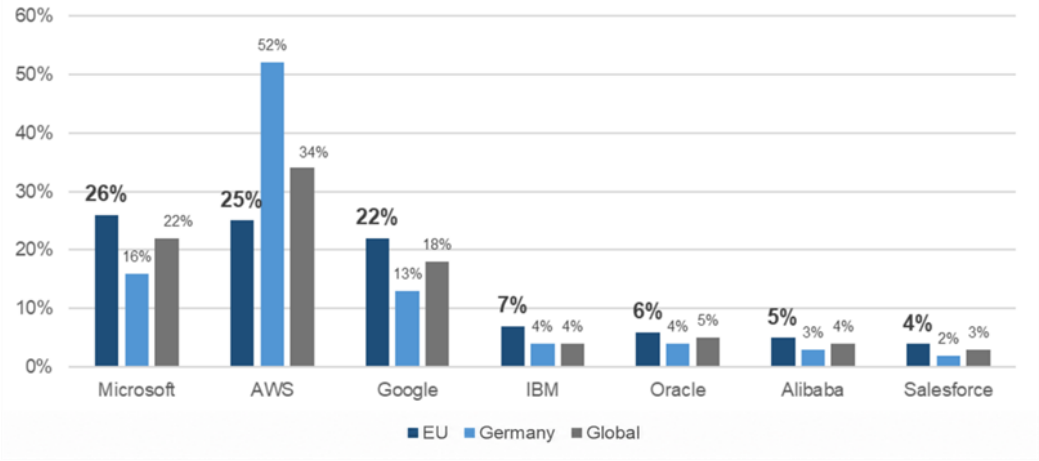
<u>Niche / specialised providers:</u>

80 See Hermann (2025): *A Reality Check on European Cloud Alternatives*; retrievable at: https://www.linkedin.com/pulse/leave-room-reality-check-european-cloud-alternatives-benjamin-hermann-nm4pe/ [8 June 2026].
81 See https://technologychecker.io/blog/cloud-provider-traffic-share [7 June 2026].
82 See IDC MarketScape: European Public Cloud IaaS 2024 Vendor Assessment; https://www.ionos-group.com/fileadmin/newsroom/EUR151035423e_IONOS.pdf [7 June 2026].
83 See https://geschaeftskunden.telekom.de/business/loesungen/digitalisierung/it-infrastructure/cloud-infrastructure/open-telekom-cloud [7 June 2026].

- **Deutsche Telekom**
- **Hetzner**
- **Ionos**
- **OVHcloud**

4.1.3 The PaaS market

Figure 4-4: Participants on the PaaS market



Source: own illustration; data source: Statista

The PaaS market in the EU has a volume of approximately €47 billion, which is equivalent to a share of 27% of the total EU cloud market. The PaaS market in the EU therefore has above-average significance compared with the global share of PaaS in the cloud market (22%).

The top three providers in the EU PaaS market are identical with those in the IaaS market, but in a different order: Microsoft is the leading provider with 26%, closely followed by AWS with 25%. Google comes third with a market share of 22%. The top three are therefore very close to each other. Together they account for 73%, which is slightly below the figure in the IaaS market (74%). The breakdown of the market shares of the top three in the EU deviates substantially from the global breakdown in the PaaS market: AWS clearly leads here with 34%, followed by Microsoft with 22% and Google with 18%. The position of AWS is particularly strong in Germany: 52% of the market here is attributable to AWS alone, followed by Microsoft with 16% and Google with 13%.

Further providers with relevant market shares include **IBM** (EU: 7%; global: 4%; Germany: 4%), **Oracle** (EU: 6%; global: 5%; Germany: 4%), **Alibaba** (EU: 5%; global: 4%; Germany: 3%) and **Salesforce** (EU: 4%; global: 3%; Germany: 2%).

Furthermore, apart from the general purpose PaaS services, above all **SAP** is relevant in the EU with its Business Technology Platform (BTP). Through the BTP, SAP has a strong

position in the enterprise PaaS market, especially with regard to the PaaS-based integration of central business processes. SAP is for this reason classified by Gartner as a "leader" in the area of "Integration Platform as a Service". According to Gartner, most customers are large and medium-sized organisations that frequently have complex production and/or logistics processes.[84]

One PaaS niche provider in the EU that according to Gartner is considered leading in the area of low-code application platforms is **Mendix**. Mendix was founded as a start-up in the Netherlands has been part of the Siemens Group since 2018. Its platform addresses industrial value chains in a targeted manner by acting as an interface between IT and machine control (OT). Mendix accordingly positions itself as a specialised low-code provider in the industry segment and is also listed by Gartner as a leader in the field of "enterprise low-code application platforms".[85]

Red Hat is particularly interesting with regard to the topic of switching cloud providers as a PaaS provider in the European market. With OpenShift, the US company offers a standardised, Kubernetes-based platform layer that can structurally reduce the dependence on individual cloud providers. Although the top three providers (AWS, Microsoft and Google) also use Kubernetes, this is typically embedded in proprietary cloud ecosystems enabling lock-in effects to continue. By contrast, OpenShift works as a cloud-agnostic abstraction layer that operates across different infrastructures, thereby facilitating multi-cloud strategies. Gartner lists Red Hat as a leader in the field of "cloud-native application platforms".[86]

The largest providers on the EU market:

- **Alibaba**
- **AWS**
- **Google**
- **IBM**
- **Microsoft**
- **Oracle**
- **Salesforce**

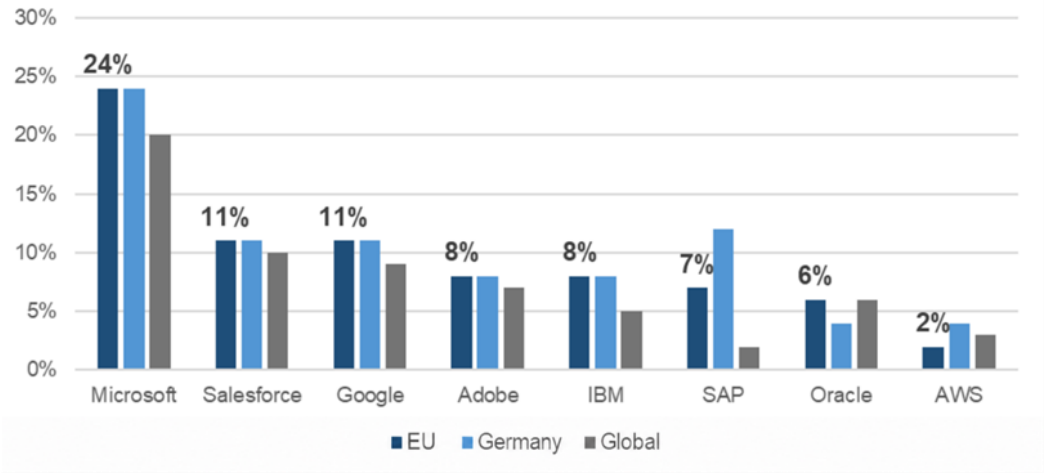
Niche / specialised providers on the EU market:

- **Mendix**
- **Red Hat**
- **SAP**

84 See https://www.gartner.com/doc/reprints?id=1-2N088GKM&ct=260318&st=sb [7 June 2026].
85 See https://www.gartner.com/doc/reprints?id=1-2LJ2SZQ2&ct=250725&st=sb; [7 June 2026] and https://www.computer-automation.de/produktionssoftware/interview-mit-raymond-kok--mendix--low-code-im-wandel.htm [7 June 2026].
86 See https://www.gartner.com/doc/reprints?id=1-2LLD11OH&ct=250801&st=sb [7 June 2026].

4.1.4 The SaaS market

Figure 4-5: Participants on the SaaS market



Source: own illustration; data source: Statista

The SaaS market has a volume of around €79 billion in the EU. With a share of approximately 45% of the total cloud market, SaaS is therefore by far the largest submarket. The same also applies to the global market, where the share lies at around 43%. The share in Germany is even higher at 55%.

The SaaS market is not only the largest submarket, but also the least concentrated one with regard to market shares. The market leader in the EU is **Microsoft** with a share of 24%, followed by **Salesforce** and **Google** with 11% each. Together the top three therefore have a market share of less than 50%. The distribution of the market shares of the top three on the global market is similar: Microsoft has a share of 20%, Salesforce 10% and Google 9%. It is interesting with regard to the German market to note that **SAP** comes second here with a market share of 12% (EU: 7%; global: 3%). Microsoft is likewise market leader on the German market with 24%. Third place is shared by Salesforce and Google with 11% each.

Further SaaS providers with relevant market shares include **IBM** (EU: 8%; global: 5%; Germany: 8%), **Adobe Cloud** (EU: 8%; global: 7%; Germany: 8%); **Oracle** (EU: 6%; global: 6%; Germany: 4%) and **AWS** (EU: 2%; global: 3%; Germany: 4%).

One specialised provider in the European SaaS market that has gained importance particularly in the area of data-driven process optimisation is **Celonis**. Founded in Germany, the company has positioned itself with its software for process mining and execution management in an independent category that is functionally located between classical business intelligence and operational process control. Based on data from existing systems such as SAP or Salesforce, Celonis enables companies to make actual

processes transparent, identify inefficiencies and increasingly also address them in an automated manner.

The SaaS services of Celonis operate as a complementary layer across existing enterprise systems and thus do not constitute a direct substitution but a functional expansion of existing structures. Celonis is classified by market observers such as Gartner as a leading provider in the field of process mining.[87] Viewed overall, Celonis therefore constitutes an example of a European SaaS provider that has successfully established itself in a highly specialised but strategically crucial niche.

By contrast, **Workday** has established itself as a leading SaaS provider in the area of human capital management (HCM). The US company offers integrated applications for HR management, payroll, talent management and financial processes, thereby positioning itself as a specialised alternative to classical ERP systems, particularly in competition with SAP. Proof of its strong positioning is its classification by Gartner as a "leader" in the field of HCM suites.[88]

ServiceNow is a provider on the European market specialised in the field of IT service management (ITSM). The US company has established itself as a leading provider in this segment and is considered in many large organisations to be the de facto standard for the management and control of IT services. Its platform in particular facilitates the structured processing of IT incidents, service requests and changes as well as the standardisation and automation of corresponding processes. ServiceNow is the only company listed by Gartner as a leader in the field of AI applications in IT service management.[89]

The largest providers on the EU market for SaaS:

- **Adobe Cloud**
- **AWS**
- **Google**
- **IBM**
- **Microsoft**
- **Oracle**
- **Salesforce**
- **SAP**

87 See https://www.gartner.com/doc/reprints?id=1-2KTK6L8K&ct=250421&st=sb/ [7 June 2026].
88 See https://www.gartner.com/doc/reprints?id=1-2LUEY765&ct=250909&st=sb [7 June 2026].
89 See https://www.gartner.com/doc/reprints?id=1-2LS73XWW&ct=250902&st=sb [7 June 2026].

Niche / specialised providers on the EU market for SaaS:

- **Celonis**
- **ServiceNow**
- **Workday**

4.1.5 Condensed overview of the identified cloud providers in the EU

The aggregated analysis of the three submarkets results in the list below with a total of 19 providers. Those submarkets are marked in green in which the respective company has a core market. Those submarkets are marked with a circle in which the company is active but which do not represent a core market of the provider. Those submarkets are marked with a dash in which the company is barely or not active at all. The table additionally shows in which country the company has its head office and, in the case of non-European providers, where the European headquarters are located (“EU HQ”).

The table shows that the IaaS, PaaS and SaaS markets each have 10 providers that identify them as a core market. The choice of provider is thus spread evenly across the service models. Geographically the distribution is such that a little more than half the companies have their head office in the USA (10), especially including the particularly large providers (Amazon, Google, Microsoft). Five of the 19 companies (approximately 26%) are headquartered in Germany. Germany is therefore overrepresented in comparison with global total cloud market shares. This is because a stronger focus was placed on German providers in the selection of specialised / niche providers. The remaining companies are split across China (2), France (1) and the Netherlands (1).

The data processing services of these providers are classified below in the classification model presented in section 3.

Figure 4-6: Aggregated overview of the identified providers

Company	Head office	IaaS	PaaS	SaaS
Adobe	USA (EU HQ: IRL)	–	o	✓
Alibaba	CHN (EU HQ: IRL)	✓	✓	–
AWS	USA (EU HQ: LUX)	✓	✓	o
Celonis	GER (Munich)	–	–	✓
Dt. Telekom	GER (Bonn)	✓	o	–
Google	USA (EU HQ: IRL)	✓	✓	✓
Hetzner	GER (Gunzenhausen)	✓	–	–
Huawei	CHN (EU HQ: GER)	✓	o	–
IBM	USA (EU HQ: IRL)	✓	✓	✓
IONOS	GER (Montabaur)	✓	o	o
Mendix	NED (Rotterdam)	–	✓	o
Microsoft	USA (EU HQ: IRL)	✓	✓	✓
Oracle	USA (EU HQ: NED)	o	✓	✓
OVHcloud	FRA (Roubaix)	✓	o	–
Red Hat	USA (EU HQ: CZE)	–	✓	–
SAP	GER (Walldorf)	–	✓	✓
Salesforce	USA (EU HQ: IRL)	–	✓	✓
ServiceNow	USA (EU HQ: IRL)	–	o	✓
Workday	USA (EU HQ: IRL)	–	–	✓
	Total:	10	10	10

Source: WIK (own illustration)

4.2 Identification and classification of the data processing services of the identified providers

In order to identify the relevant data processing services of the key cloud providers, recourse is made to the automated extraction and analysis of data from websites (web scraping). This enables specific cloud service names and descriptions as well as metadata (URLs, time of retrieval) to be transparently compiled from official sources in a structured manner.

In order to depict as comprehensive an overall picture of the current cloud service landscape as possible, information is obtained via three approaches.

1. **Structured APIs or index endpoints:** if a provider supplies a machine-readable service index, this is used as the primary source for identifying and describing provider services. It offers the most complete and consistent data corpus. **AWS**, for example, offers a public pricing index API that indexes all billing-relevant services in a machine-readable manner. **Google Cloud** provides the GCP Discovery API that publishes around 300 service names; the terms of service page additionally provides descriptions of services. **IBM Cloud** offers the Global Catalog API that contains all service types (service, platform_service, composite).

Microsoft Azure offers two public APIs: the MS Learn Catalog API and the Azure Retail Prices API. **SAP** uses an internal content management system API that provides the structured product portfolio in a machine-readable format.

2. **Official site maps of cloud services:** should no structured API exist, the site map of the cloud services offered by the provider is headed for (eg *URLs with /products/, /services/, /solutions/*) as this normally pools all information about services. The specific page layout varies significantly between the providers.
3. **Individual service sites (landing pages):** should it exist, the proprietary canonical service URL for each individually identified service is downloaded to extract from this the specific service description and category that is frequently missing on the site map.

Table 4-1: Primary sources concerning the services of cloud providers

Provider	Primary source
Adobe	Product sites
Alibaba Cloud	Websites & documentation
AWS	API & price lists & websites
Celonis	Websites & PDF catalogue
Deutsche Telekom	Site maps (index pages) and individual product sites
Google Cloud	API & websites
Hetzner	Individual product sites
Huawei Cloud	Individual product sites (landing pages)
IBM Cloud	API & websites
IONOS	Site maps & category pages
Mendix	Websites
Microsoft Azure	API and price data
Oracle	Websites
OVHcloud	Price & category pages
Red Hat	Individual product sites
Salesforce	Websites
SAP	API
ServiceNow	Product list and individual product sites
Workday	Product sites & backup catalogue

Source: WIK, own illustration

As providers structure their product sites very differently, different strategies are deployed for various page types, such as tables, card layouts, text pages or tabs. As websites contain a lot of other content in addition to product information (eg navigation elements, marketing texts or documentation pages), this is removed as far as possible using multiple filters. These include:

- excluding typical navigation, documentation and marketing elements,
- filtering out unsuitable or clearly not product-related descriptions (eg filler words or very short, very long or typical section headings),
- removing non-meaningful standard texts (eg cookie, contact or copyright notices) and
- merging duplicates.

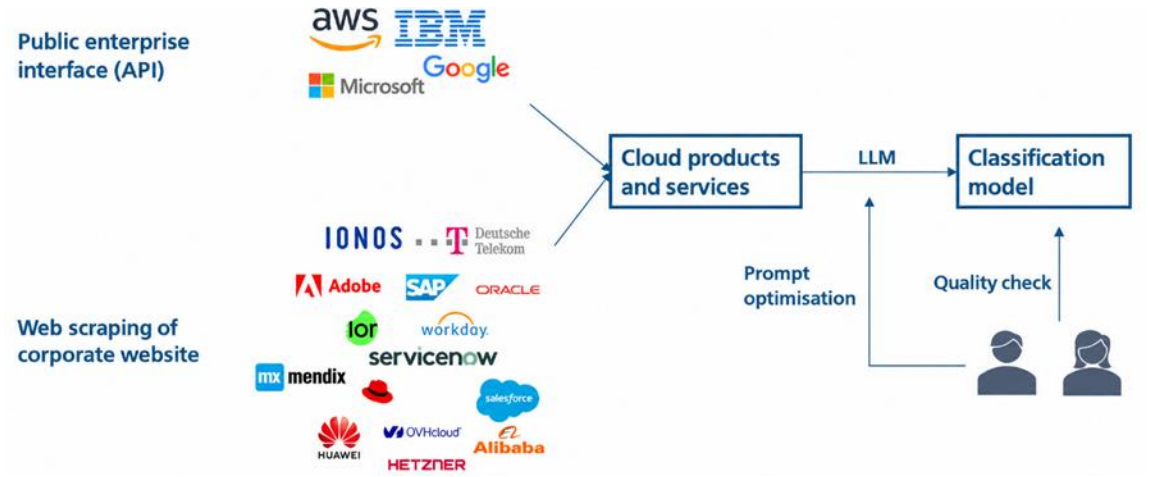
However, the final result will not be entirely purged and a certain degree of “noise” (irrelevant hits) will still remain after filtering. To further reduce irrelevant results and classify the identified data processing services using the classification model, modern high-performance large language models (LLMs) are deployed as described in the following section.

4.3 Classification of the identified data processing services using the classification model

Application of the classification model

The classification model set out in section 3 (Table 3-2) serves as the basis for classifying the individual cloud services. A large language model (LLM) is used to match the identified cloud services to the classification model. Clear rules are defined beforehand by which the LLM must be guided to keep its susceptibility to error as low as possible. The deployment of an LLM makes particular sense in this context as it is capable of efficiently processing and semantically classifying large volumes of heterogeneous service names and descriptions, thereby facilitating consistent and scalable allocation in the classification model. The underlying prompts to the LLM are gradually adjusted and refined after reviewing the model’s output results across multiple iterations to ensure an accurate classification.

Figure 4-7: Classification of the identified data processing services using the classification model



Source: WIK, own illustration

The following must be taken into account during processing:

- Fixed categories must be adopted literally from the classification model and may not be modified by the LLM:
  - *service_model:* service model of the service (eg IaaS, PaaS, SaaS, IaaS/PaaS, …)
  - *main_objective*: overriding processing objective (PD = processing of data, SRD = storage, retrieval & delivery, TD = transformation & development, DF = data foundation)
  - *main_function*: primary technical function of the category (eg virtual infrastructure, data warehouse, managed Kubernetes, …)
- Variable categories can be adjusted by the LLM if necessary but follow the structural composition of the model:
  - *level_0* from the classification model – superordinate domains (eg compute, storage, AI & machine learning, …)
  - *level_1* - 1: subdomain (eg virtual infrastructure, managed orchestration, …)
  - level_2 - 2: subdomain (eg virtual machine hosting, object storage, …)
- In addition, the specific technical interface (portability_spec) via which this service is portable (eg Kubernetes API / manifest, S3 REST API, SAML / OIDC federation endpoint) is documented by the LLM. This takes place individually for each classified service based on the available information about a service and is not adopted from the taxonomy.

LLM-supported classification

Classification of the compiled services in the classification model takes place automatically by means of a rule-based LLM framework. The classification is carried out in groups (batches) of eight services each, with a temperature of 0.1 configured for the language model. The temperature governs how much the model varies between different possible answers: low temperatures lead to more consistent and reproducible results, while higher temperatures generate more randomness and different wordings. The selected temperature of 0.1 therefore ensures that the model makes practically identical classification decisions for the same input.

Each service is analysed prior to classification to determine whether it is demonstrably billing-relevant (eg from the AWS Pricing Index or Azure Retail Prices API). Such a service may never be marked by the LLP as out of scope and must be classified to the taxonomy. If there is no information available about billing, the three verification steps set out below are carried out successively for classifying the service.

The LLM receives the full taxonomy block (all entries in the format [service_model] obj=... | fn=... | level_0 → level_1 → level_2 | portability: ...) and the service name and description and delivers one of three classification results in return for each service:

1. **Taxonomy match (within the taxonomy and not outside the scope of application of the Data Act)**

The service is assigned to the most similar taxonomy entry. An exact match is not imperative; functional approximations are expressly envisaged. As already described above, the service model, main objective and main functionality are adopted literally from the taxonomy. The level_0, level_1 and level_2 gradings are adjusted by the LLM to the specific service but follow the taxonomy structure. The specific technical interface is individually generated by the LLM for each service. Cloud services without a sufficient description are assigned to the next broader suitable category through generalisation and marked with “low confidence”.

2. **Taxonomy gap (outside the taxonomy but not outside the scope of application of the Data Act)**

These are services for which no acceptable functional match exists after conducting a full analysis of all taxonomy entries. However, this concerns an existing data processing service. In this case the LLM generates suggestions for categorisation and the specific technical interface.

3. **Out of scope (outside the taxonomy and outside the scope of application of the Data Act)**

A service is only marked as out of scope if it does not constitute an independent billable data processing endpoint through which customer data flow. Typical out-of-scope categories are remnants of web scraping, billing constructs (support plans, credit programmes), SDK/CLI list entries without proprietary cloud endpoint, educational resources (certification programmes, documentation portals), one-off migration tools, pure preview/beta entries, marketing claims and navigation labels, and localisation entries.

Confidence assessment

Each classification receives a three-tiered confidence label from the LLM that indicates the reliability of the classification for downstream manual review:

- **High:** strong functional match; the service name or service description clearly support the classification.
- **Medium:** reasonable match; slight ambiguity but justified classification to taxonomy.
- **Low:** poor or no description; the LLM has generalised to the next broader general category.

Table 4-2: Assessment of the services of cloud providers

Provider	Overall	Within the taxonomy	Share (%)	Outside the taxonomy	Out of scope / noise
Google Cloud	494	393	80%	36	65
Microsoft Azure	288	248	86%	7	33
IBM Cloud	266	221	83%	35	10
SAP	259	250	97%	0	9
AWS	251	207	82%	44	0
Oracle	208	194	93%	0	14
Alibaba Cloud	198	185	93%	13	0
ServiceNow	185	164	89%	5	16
Huawei Cloud	145	124	86%	10	11
Adobe	137	102	74%	6	29
Salesforce	136	102	75%	0	34
OVHcloud	75	63	84%	4	8
Celonis	74	62	84%	12	0
Deutsche Telekom	72	68	94%	4	0
IONOS Cloud	52	45	87%	7	0
Mendix	47	37	79%	0	10
Red Hat	40	40	100%	0	0
Hetzner	22	17	77%	5	0
Workday	15	14	93%	1	0
Total	2,964	2,536	87%	189	239

Source: WIK, own illustration

The taxonomy match rate of around 87% across all providers shows that the developed classification model covers the overriding majority of commercial cloud data processing services. However, a small portion of the classified services still contains incorrect data as it is not possible despite the use of web scraping and modern LLMs to say for certain whether all extracted entries actually are genuine products. Differences in website layout and documentation of the individual cloud services of the providers impede flawless documentation, which can lead to hits that are incorrect or difficult to classify. Although this is countered by the application of confidence levels, it should nevertheless be borne in mind when interpreting the results (see Table 4-3).

Table 4-3: Breakdown of confidence levels across all services

Provider	Number of services	High confidence (%)	Medium confidence (%)	Low confidence (%)
Workday	15	53.3	40	6.7
Hetzner	22	54.5	18.2	27.3
Red Hat	40	85	12.5	2.5
Mendix	47	17	21.3	61.7
IONOS Cloud	52	65.4	15.4	19.2
Deutsche Telekom	72	72.2	20.8	6.9
Celonis	74	37.8	45.9	16.2
OVHcloud	75	70.7	13.3	16
Salesforce	136	47.1	27.9	25
Adobe	137	43.8	22.6	33.6
Huawei Cloud	145	64.8	11.7	23.4
ServiceNow	185	23.8	51.9	24.3
Alibaba Cloud	198	78.3	8.1	13.6
Oracle	208	62.5	20.7	16.8
AWS	251	47.4	11.2	41.4
SAP	259	56	35.5	8.5
IBM Cloud	266	59.8	20.7	19.5
Microsoft Azure	288	44.8	20.5	34.7
Google Cloud	494	57.5	15.2	27.3
Total	*2,964*	*54.4*	*21.7*	*24*

Source: WIK, own illustration

Altogether this approach permits the classification of more than 2,600 data processing services of the selected providers in the classification model. If the results are considered from an aggregated perspective, the overall view of the service model-main objective-main functionalities combinations of the analysed services of the cloud service providers shows that the largest providers, in particular AWS, Google Cloud, Microsoft Azure, Alibaba Cloud and Oracle, are represented in practically all areas, although the PaaS

service model with the main objective “Making available digital functions” has by far the broadest provider presence.

The results also make clear that the market is developing structurally towards PaaS. While pure IaaS categories above all represent basic infrastructure functionalities, PaaS is dominated by functional, modular and integrable services that are particularly relevant for data-driven applications, governance and automation. The strong presence of the largest providers in these PaaS categories also shows that their strategic positioning is increasingly shifting from the mere provision of computing, storage and network infrastructure to the orchestration of entire cloud ecosystems (see Table 4-4).

Table 4-4: Aggregated allocation of cloud providers investigated in the classification model

Service model	Main objective	Main functionality	Quantity	Cloud providers
IaaS	Processing of data	Virtual infrastructure	16	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, ServiceNow
IaaS	Storage and retrieval of data	Standardised data stores	10	Alibaba Cloud, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle
IaaS/PaaS	Making available digital functions	Workflow orchestration	3	AWS, Alibaba Cloud, Celonis
IaaS/PaaS	Transfer of data	Dedicated interconnect	10	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle
IaaS/PaaS	Transfer of data	Network security / VPC	13	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat
IaaS/PaaS	Transfer of data	Virtual private network (VPN)	9	Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle
IaaS/PaaS/SaaS	Making available digital functions	Desktop as a Service (VDI)	7	AWS, Alibaba Cloud, Huawei Cloud, IBM Cloud, Microsoft Azure, Oracle, ServiceNow
IaaS/SaaS	Making available digital functions	CRM	9	Adobe, Celonis, Google Cloud, IBM Cloud, Microsoft Azure, Oracle, SAP, Salesforce, ServiceNow
IaaS/SaaS	Making available digital functions	ERP/SCM	13	AWS, Adobe, Celonis, Google Cloud, Hetzner, IBM Cloud, Mendix, Microsoft Azure, Oracle, SAP, Salesforce, ServiceNow, Workday
IaaS/SaaS	Making available digital functions	HCM	10	Adobe, Alibaba Cloud, Google Cloud, IBM Cloud, Microsoft Azure, Oracle, SAP, Salesforce, ServiceNow, Workday
PaaS	Making available digital functions	API management	15	AWS, Adobe, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, Salesforce, ServiceNow
PaaS	Making available digital functions	Content delivery	12	AWS, Adobe, Alibaba Cloud, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle
PaaS	Making available digital functions	Data lakes	11	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, Microsoft Azure, Oracle, SAP, Salesforce

Service model	Main objective	Main functionality	Quantity	Cloud providers
PaaS	Making available digital functions	Data warehouse	16	AWS, Adobe, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle, SAP, Salesforce, ServiceNow, Workday
PaaS	Making available digital functions	Dev ecosystem	14	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, ServiceNow
PaaS	Making available digital functions	Enterprise messaging	14	AWS, Adobe, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, ServiceNow
PaaS	Making available digital functions	In-memory databases	9	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, Red Hat
PaaS	Making available digital functions	Intelligence services	18	AWS, Adobe, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, Salesforce, ServiceNow, Workday
PaaS	Making available digital functions	Mgmt & governance	11	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, Oracle, Red Hat, ServiceNow
PaaS	Making available digital functions	NoSQL databases	10	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, ServiceNow
PaaS	Making available digital functions	Relational databases	14	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP
PaaS	Making available digital functions	Stream processing	10	AWS, Alibaba Cloud, Celonis, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, Oracle, ServiceNow
PaaS	Making available digital functions	Workflow orchestration	15	AWS, Adobe, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, Mendix, Microsoft Azure, Oracle, SAP, Salesforce, ServiceNow, Workday
PaaS	Processing of data	Managed orchestration	13	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP
PaaS	Processing of data	Specialised compute	5	AWS, Google Cloud, IBM Cloud, Microsoft Azure, OVHcloud
PaaS	Storage and retrieval of data	Data protection & archive	12	AWS, Alibaba Cloud, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle, SAP
PaaS	Storage and retrieval of data	Standardised data stores	13	AWS, Adobe, Alibaba Cloud, Deutsche Telekom, Google Cloud, Hetzner, Huawei Cloud, IBM Cloud, IONOS Cloud, Microsoft Azure, OVHcloud, Oracle, Red Hat
PaaS/SaaS	Making available digital functions	Mgmt & governance	15	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS Cloud, Mendix, Microsoft Azure, Oracle, Red Hat, SAP, Salesforce, ServiceNow
SaaS	Making available digital functions	ESG & carbon tracking	7	Celonis, Google Cloud, IBM Cloud, Oracle, SAP, Salesforce, ServiceNow
SaaS	Making available digital functions	Managed collaboration	10	AWS, Adobe, Huawei Cloud, IONOS Cloud, Mendix, Microsoft Azure, Oracle, SAP, Salesforce, ServiceNow
SaaS/PaaS	Making available digital functions	Mgmt & governance	16	AWS, Alibaba Cloud, Celonis, Deutsche Telekom, Google Cloud, Huawei Cloud, IBM Cloud, IONOS

Service model	Main objective	Main functionality	Quantity	Cloud providers
				Cloud, Mendix, Microsoft Azure, OVHcloud, Oracle, Red Hat, SAP, Salesforce, ServiceNow

Source: WIK, own illustration

5 Analysis of practical application challenges

5.1 Distinction of non-permissible "specific support activities" from services that providers may continue to charge for

For a transitional period of three years as of the entry into force of the Data Act on 11 January 2024, providers of data processing services may impose charges for the switching process (Article 29(2) of the Data Act). These charges may not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned (Article 29(3) of the Data Act). Following the end of this transitional period as of 12 January 2027, providers of data processing services will no longer be permitted to impose any switching charges (Article 29(1) of the Data Act). Recital 88 sentence 3 cites two examples of costs caused by switching One comprises the so-called "data egress charges" for costs incurred for the transit of data from one provider to another or to an on-premises ICT infrastructure. The other comprises costs related to specific support actions during the switching process. Article 2(35) and (36) of the Data Act contains clear definitions for the first cost example, the data egress charges. This is not the case for the cost-related charges for support actions in the second example: here the delimitation from services that may continue to be charged for after 12 January 2027 is not clear. The latter particularly include standard services (recital 89 sentence 5), professional transition services (recital 85 sentence 6) and additional migration services at the customer's request (recital 89 sentence 3).

This subsection specifically aims to answer the following two questions in particular:

- Which specific support actions are providers of data processing services no longer permitted to charge their customers for as of 2027 during the switching process?
- Where is the boundary from separate services pursuant to Article 2(36) in conjunction with Article 29(1-3) of the Data Act that may continue to be charged for in the contractual phase of a switching process?

The method applied comprises desk research and the analysis of:

- EU documents: Data Act, draft non-binding standard contractual clauses for cloud computing contracts[90]
- Up-to-date market surveys and guidelines of regulatory authorities and other relevant authorities (ARCEP, CMA, BEREC)

90 European Commission, C(2025) 7750 final: Approval of the draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts (ANNEX VI: STANDARD CONTRACTUAL CLAUSES on Switching and Exit).

- Interviews with cloud providers (indications of grey zones regarding delimitation)

Delimitation criteria are ultimately to be drawn up for ensuring a consistent application of the relevant provisions of the Data Act concerning the billing of specific support actions during the switching process.

It can be concluded after consulting the relevant literature that the boundary essentially runs where a service is still part of the legally owed facilitation of switching (in which case it can no longer be billed separately as of 12 January 2027) and where it transcends this. The definition of "switching charges" in Article 2(36) of the Data Act is the prevailing factor: it covers charges that a provider imposes on a customer for the actions mandated by this Regulation for switching. Only *standard service fees* and *early termination penalties* are excluded.

On the other hand, a service may be billed separately if it is not imperative for successful and secure switching but initiated at the specific request of a customer that transcends the provisions of the Data Act. The customer must have consented to the price for these additional migration services beforehand. The following table illustrates possible delimitation criteria for support actions during the switching process.

Table 5-1: Delimitation criteria for support actions

Dimension	Specific support actions (Article 29(1-3) of the Data Act)	Separate services providers may continue to charge for
Trigger	Mandatory statutory requirement (Data Act)	Specific customer request
Nature of service	Standardised, imperative for switching	Customised, individual, optimising
Depth of development	No new development of technologies necessary	Development of specific technical solutions
Price limit (until January 2027)	Strictly capped to actual costs incurred (directly and exclusively caused by switching)	Market-based commercial rates
Price limit (as of January 2027)	**Prohibited (€0)**	Market-based commercial rates

Source: WIK-Consult

A detailed breakdown of the delimitation by category is provided by the recently published guidelines of ARCEP.[91] These were published as a result of the public market consultation conducted in 2024[92] under consideration of the comments received. The following main categories and subcategories of support action are defined on this basis:

91 ARCEP (2026): CONSULTATION PUBLIQUE, Projet de lignes directrices portant sur les coûts susceptibles d'être pris en compte dans la détermination des frais de changement de fournisseur de services d'informatique en nuage autres que les frais liés au transfert de données.

92 ARCEP (2024): CONSULTATION PUBLIQUE, Régulation des services d'informatique en nuage (cloud): Faciliter le changement de fournisseurs de services cloud et la mise en œuvre d'architectures multi-cloud grâce à un nouvel encadrement tarifaire et technique.

Actions counting as switching charges (prohibited from 12 January 2027)

These services fall under the obligation of the original provider to support the switching process. If they were to be denied, this would impede the switch.

- Reasonable assistance: this comprises actions that ensure the switch takes place successfully, efficiently and securely. These include:
    - Technical support with difficulties during switching, including causal analysis and troubleshooting in the environment of the original provider.
    - Data processing for extraction: preparation of the data for export in a conventional, machine-readable format and verification of the completeness and integrity of the extracted data.
    - Conducting of tests: support of the customer with tests to verify the proper functioning of data export and the integrity of the data at the end of the process.
    - Provision of specific technical documentation containing all necessary information for carrying out the switch.
- Provision of tools and resources:
    - Use or provision of software tools for data export or data transformation.
    - Temporary data storage: storage of a copy of the data during the switching procedure if this is necessary due to technical constraints for implementation.
- Upholding of security: measures to extend the security level that the provider has contractually undertaken to uphold to cover all technical arrangements during the entire switching process (eg network connections).

Services that may continue to be charged for

These include services that transcend the statutory obligations of the provider to facilitate switching or form part of regular operation.

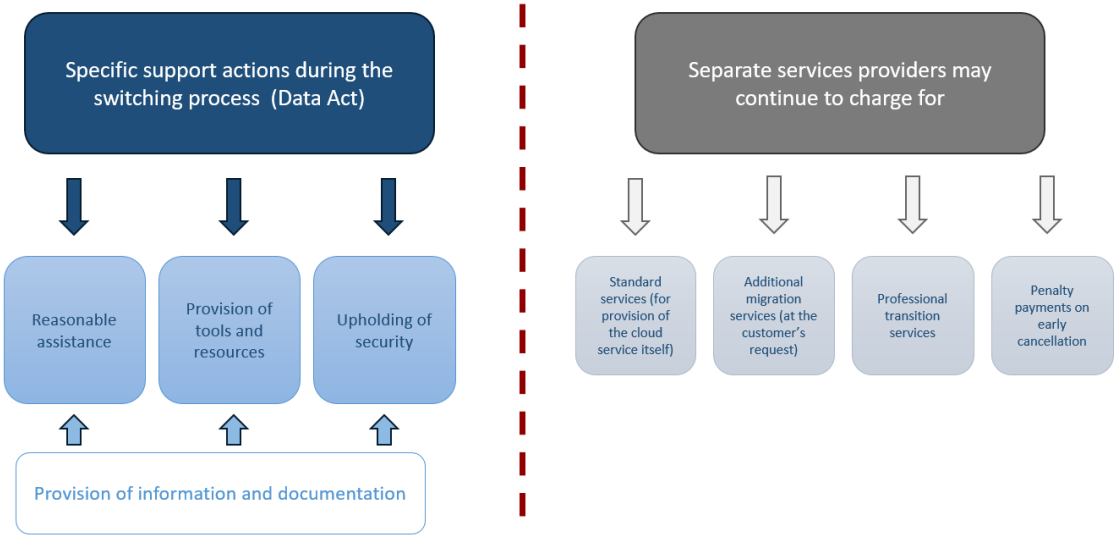
- Standard services: the regular charges for provision of the cloud service itself remain unchanged. The contract remains in force during the transitional period and the ongoing charges for the capacities used remain payable.
- Additional migration services (at the customer's request): these are services that go beyond the requirements of the Data Act and have been explicitly requested by the customer. According to ARCEP, examples include:
    - Audits of information systems and customer data.
    - In-depth needs assessments and personalised consulting in the context of the migration project.

- Services for planning and management of the migration project (project management).
- Amendment of scripts or code parts to adjust the migrated services to the specific configuration of the target provider.
- Training for the new tools and the target provider's environment.
- Security services that go beyond the level of the existing contract.

- Professional transition services: while the original provider is responsible for extraction, the uploading of the data to the new environment falls in the responsibility of the customer or target provider unless a specific professional transition service is agreed.

The following illustration summarises the categories listed above:

Figure 5-1: Delimitation and categories of actions



Source: WIK-Consult

In summary, it can be said that everything the provider is required to do to ensure the customer is technically able to extract its data and leave the service securely falls under switching charges (that are prohibited from 2027). Everything going beyond this (such as consulting, code amendment or project management) remains liable for remuneration as an additional service.

5.2 Interpretation of the exemption provisions set out in Article 31 of the Data Act

Article 31 of the Data Act reads as follows:

Article 31

Specific regime for certain data processing services

(1) The obligations laid down in Article 23, point (d), Article 29 and Article 30(1) and (3) shall not apply to data processing services of which ***the majority of main features*** *has been custom-built to accommodate the special needs of an individual customer or where all components have been developed for the purposes of an individual customer, and where those data processing services are* ***not*** *offered* ***at broad commercial scale*** *via the service catalogue of the provider of data processing services.*

(2) The obligations laid down in this Chapter shall not apply to data processing services provided as a non-production version for testing and evaluation purposes and for a limited period of time.

(3) Prior to the conclusion of a contract on the provision of data processing services referred to in this Article, the provider of data processing services shall inform the prospective customer of the obligations of this Chapter that do not apply.

Article 31(1) of the Data Act serves to distinguish individually developed data processing services (for individual customers) from standardised services offered on a broad commercial scale. The provision is systematically contained in Chapter VI of the Data Act that aims to reduce barriers to switching for standardised data processing services (eg cloud and platform services). According to this provision, individually customised solutions developed specifically for a customer are to be subject to regulatory requirements to a reduced degree.

a) How is the indeterminate legal concept "majority of main features" (Article 31(1) of the Data Act) to be interpreted?

The term **"majority of main features"** constitutes an indeterminate legal concept. The concept of main feature is understood here to be equivalent to the concept of main functionality within the meaning of Article 2(9) of the Data Act. Despite the use of varying terminology, namely "main functionalities" in Article 2(9) of the Data Act and "main features" in Article 31(1) of the Data Act, this is considered in the present case merely to be due to an editorial error. An overview of potential main functionalities can be found in the classification model in section 3.

The literature has already dealt in part with the definition of the legal concept of "the majority of main features".[93] It is thought that a feature should generally be considered "main" if it is of fundamental importance for the service or constitutes its core task. In this respect, the **main feature** regularly defines the actual benefit of the service for the customer.[94] It comprises the essential modules or processes of a data processing system

93 See Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 3 et seq.
94 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 5.

without which the service would be unable to fulfil its basic function. This supports the aforementioned understanding of the main feature as synonymous with main functionality. According to this interpretation, a service can also contain multiple main functionalities or features in addition to secondary functionalities. If a service fulfils two or more main features, the focus must be placed on the majority proportion of the agreed main functionalities.

The present case is therefore about the **functional components without which the service would not fulfil its purpose** and **not about mere secondary features (such as interfaces or security features) that consequently do not have to be developed individually for the needs of a customer, but can also be adopted from existing databases**.

Examples: the main features of a data processing service typically include in particular the actual data processing and business logic, analysis or AI modules, central data storage and the management of workflows. These features regularly determine the actual purpose and added value of a system. One example of this is a platform developed individually for an automotive manufacturer for the analysis of production data for which the central logic for the processing of sensor data from production facilities is specifically tailored to the production processes of this company. The actual data processing for the detection of quality deviations or optimisation of production parameters would be a customer-specific core function in such a case. Another example is a customised AI solution that is combined with company-related historic data, traffic flows and weather information to facilitate a dynamic optimisation of supply chains in the future. If such an algorithm were developed specifically for a company and not distributed as a general product, it would constitute an individually developed main feature of the service.

Negative delineation: on the other hand, merely **superficial adjustments**, such as adjustments to user interfaces, branding, dashboards or report templates, do not qualify as main features as they do not determine the basic functioning of the data processing service. See sentence 5 et seq. concerning the concept of custom-built features. The same applies to mere **supporting elements or secondary features** (eg additional interfaces, supplement to individual configuration parameters, establishment of further backup features).

Supplementary consideration: the concept of main functionality pursuant to the classification model in section 3 (determination of the same service type) could be drawn on for classifying corresponding main features. It must be borne in mind here that a data processing service can fulfil multiple functionalities simultaneously and which of these are to be considered main features depends on the specific use case.

The **quantitative threshold** implied in the provision **("the majority") of main features** likewise requires clarification. The question therefore arises as to **when the requirement**

is met for "the majority" of main features to be tailored to the specific needs of an individual customer.

There is currently a varying mood emerging in the literature with regard to this question. The only point on which there is agreement is that merely customising a standardised data processing service does not suffice.[95] The provision is understood in some of the literature as meaning "that at least 75% of the main features of a service must be tailored to the specific needs of an individual customer to benefit from the reduced obligations".[96] The expression "majority" is equated by these voices "with an overwhelming majority".[97] It is this understanding that underlies the German language version. The view is also represented in the literature that "a threshold of 50%" can fulfil the requirement of most features.[98] The core justification of this reading is derived from the English language version of Article 31 of the Data Act.[99] This "phrase 'the majority of main features' corresponds in this respect to a simple and not a qualified majority (similarly to the French ['majorité'] and the Spanish ['major'])".[100] The understanding geared to a simple majority of features (fundamentally >50%) is convincing. The decisive factor is therefore whether a majority of the functional core components of a service have been developed or significantly amended specifically for an individual customer. The specific delimitation of the functional scope is already posing challenges in practice for the supervisory authority. In addition to the other language versions, the purpose of the provision also speaks in favour of this interpretation.[101] This is specifically aimed at creating a fair balance between the interests of providers and customers of the data processing service. Based on this privilege, providers of customer-specific services are not to be subject to the same extensive obligations drawn up for standardised services. Providers could otherwise consider themselves impeded in offering customer-specific solutions.[102] The interpretation of the provision presented here could additionally strengthen the willingness of service providers to develop individual solutions without placing a disproportionate burden on them in doing so.[103] A threshold based on a majority accordingly corresponds "not only to the purpose of the provision, but additionally also creates a practical regulatory framework".[104]

---

95 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 6; BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 14; SPS Der neue Data Act Art. 6 side note 43; Pommerening/Nickel RDi 2024, 289 (292); probably also Sattler CR 2024, 213 (214).

96 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 7.

97 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 7; with reference to BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 14.

98 SPS Der neue Data Act Art. 6 side note 44; Pommerening/Nickel RDi 2024, 289 (292); essentially also applies to BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 14.

99 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 7; BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 14.

100 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 7; BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 14.

101 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 7 et seq.

102 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 8.

103 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 8.

104 Monschke/Lauterbach, in: Paschke/Schumacher, Data Act, Art. 31 side note 8.

How this majority of features is determined in each individual case is the responsibility of the supervisory authority. This assessment is not merely quantitative, but also qualitative: rather than a purely technical consideration, a contractual-functional perspective must be adopted here. This therefore comes down especially to the agreed deployment of features as exercised in practice and not to whether the features require the greatest computing power or the like or possess the proportionately longest code. The supervisory authority must particularly take the following criteria into account here: the total number of main functionalities, the scope of use of the individual main functionalities and the overall importance of the respective main functionalities. The importance of the respective main functionalities can be determined in particular on the basis of their technical, organisational and economic significance. Decisive factors here include the complexity of the functionality, the number of users affected, the frequency and duration of its use, its importance for the overall operation of the service and the outlay required for its development, provision and maintenance. While the development outlay is not decisive when viewed in isolation, it can be taken into account as an indication of the complexity and importance of a main functionality. This assessment must be carried out in each individual case.

Example 1: a comparatively clear case is posed by an individually developed data platform created from multiple components: 1) the platform stores data individually for this company in the form of proprietary software protocols, 2) the central production optimisation algorithm and 3) a special AI model for predictive maintenance have been programmed for this company, 4) the visualisation components (via Tableau or Grafana) and 5) data hosting (via MongoDB, PostgreSQL or a proprietary solution) are based on a standard solution. The standard solution can be a proprietary solution distributed to a large number of customers or a standardised module from a library or framework. Three out of five main feature areas are configured in a customer-specific manner in this example and their significance from an overall perspective also prevails. “The majority of main features” in such a case would be tailored to the needs of an individual customer.

Example 2: by contrast, a borderline case can exist for a data platform comprised of five main functionalities of which only two have been individually developed but where these functionalities are so decisive in terms of their importance that this must nonetheless be taken into account in the overall view. This data platform consists of: 1) data integration, 2) product optimisation, 3) predictive maintenance, 4) visualisation and 5) data hosting. Two of these functionalities, the production optimisation algorithm and the AI model for predictive maintenance, have been individually developed for a specific customer. The other functionalities are based on standard solutions. Classification in such a case does not depend on a merely quantitative consideration. Instead, the decisive factor is what functional significance the individually developed components have for the overall product. If the production optimisation algorithm and the predictive maintenance model form the technical and economic core of the platform, while visualisation, hosting and data integration merely fulfil supportive, replaceable or customary market functions, these

two individually developed functionalities can represent the majority of main features despite their lower quantity. In this case the platform can be viewed overall as predominantly tailored to the needs of an individual customer.

Other borderline cases are also conceivable in which the individually developed main functionalities prevail quantitatively, but the actual focus of the service lies on the qualitatively more important off-the-shelf main functionalities. The "majority of main features" in such a case would therefore be classified as an off-the-shelf solution rather than as "tailored to the needs of the individual customer".

Negative delineation: the requirement is generally not met if a **standardised cloud or software service is merely configured or supplementary services from a standardised product range can be additionally booked** (eg various standardised software modules from libraries or frameworks). The same applies if the service is **adjusted** by the provider or the customer themselves only **(marginally) within the scope of the components offered**. It is common practice for data processing services to draw on such recyclable components and not to develop corresponding functionalities individually.

If, for example, a company makes use of a generally available cloud analytics service merely requiring dashboards to be adjusted, access rights configured or own data sources integrated, the main features (= data analysis, data processing or model libraries) will remain part of a standardised product. These cases do not comprise a service for which the majority of main features have been developed in a customer-specific manner. This requirement is likewise not met with classical Software-as-a-Service products for which a standard platform is used that can be supplemented with additional plug-ins, reports or interfaces. White label models for which only individual elements or the user interface are adjusted, while the underlying technical architecture and processing remain unchanged, also do not essentially constitute services with main features predominantly designed in a customer-specific manner.

Concept	Explanation
"main features"	**Core task (significant modules or processes) of a data processing service; a service can have multiple features;** see also the concept of main functionality AP 2.
"the majority"	The decisive factor is whether **more than half of the functional core components** of a data processing service have been developed or significantly amended specifically for an individual customer. The supervisory authority is responsible for determining this in each individual case (see above).

b) How is the indeterminate legal concept "broad commercial scale" (Article 31(1) of the Data Act) specifically to be interpreted?

The criterion *"where those data processing services are **not** offered **at broad commercial scale** via the service catalogue of the provider of data processing services"*

serves to distinguish between individually developed solutions and standardised data processing services distributed as regular market offerings. The legislator's intention with this provision is for customised individual developments that are typically only drawn up for a single client not to be subject to the same regulatory requirements as standardised cloud or platform services.

The indeterminate legal concept "broad commercial scale" is to be interpreted functionally and relates to whether a data processing service is actively distributed on the market as a standardised product or service. The decisive factor here in particular is whether the service is offered multiple times and to an indefinite multitude of customers.[105]

A broad commercial scale therefore normally exists if a provider in particular:

1) systematically markets a data processing service,[106]

2) offers a data processing service via a public service catalogue or a product portfolio, or

3) provides a data processing service for multiple customers.

This list is not exhaustive. Should such a market orientation be lacking, this speaks against a broad commercial scale.

The following criteria in particular can be drawn on for the official legal application:

Criterion	Meaning
Standardisation	The service is based to an overriding extent on a standardised product or a platform that can be used by different customers.
Market offering	The service is actively offered via a product catalogue, a website or distribution structures.
Repeated selling	The provider intends to distribute the service multiple times with an identical or largely identical functionality (sale, rent, lease).
Scalability	The architecture is designed to serve a large number of customers simultaneously. This criterion alone does not suffice for the assumption of a broad commercial scale; see recital 98 sentence 4.

105 Specht/Hennemann/Linardatos, DA/DGA, second edition, Art. 31 side note 11 criticises the fact that this wording puts initial customers in a worse position than potential future customers if the product is rolled out on the market in a scaled manner. However, this can be answered by pointing out that the initial customer was able to contribute decisively to the product's development and have a say in the individual functionalities in accordance with its needs. In addition, according to BeckOK Datenschutzrecht/Schmidt-Wudy Data Act, 55th edition, Art. 31, side note 19, this preferential treatment by the service provider of all customers and therefore also of the initial user ceases to apply when the same product is ready for market, promoted, has been included in the provider's service catalogue and is distributed to a multitude of further customers.

106 BeckOK Datenschutzrecht/Schmidt-Wudy Data Act, 55th edition, Art. 31, side note 18 appears to focus primarily on the advertising element on the market.

The more pronounced the aforementioned criteria are, the more likely a broad commercial scale is to exist.

Examples of a broad commercial scale in this connection: cloud services that were originally developed for one customer and are now to be provisioned on the market in a scaled manner owing to demand. A data analysis platform that was initially developed and provided free of charge as a test version for individual customers and is now being included and scaled in the product portfolio. An AI or data platform that is currently only used in Europe by a small number of exclusive customers but is already marketable in other regions and structurally designed to be used by a large number of customers.

A broad commercial scale **does not exist** if a data processing service is uniquely developed for a customer as part of an individual project, the provider does not have any intention of offering the solution to further customers or the technical architecture is tailored exclusively to the specific IT environment of an individual customer.

This condition should thus apply to and exclude from the privilege contained in Article 31(1) of the Data Act those data processing services that are broadly promoted by the company and scalable but have not yet established themselves on the market and are therefore only used by a small number of individual customers (limited take-up rate).

Overall assessment:

The requirement of a “broad commercial scale” must be assessed **cumulatively** with the other requirements of Article 31(1) of the Data Act. The exception from the obligations of Chapter VI therefore only applies if:

1) the majority of main features are tailored to the needs of an individual customer **or** all components have been developed for an individual customer, **and**

2) the service is **not** offered **at broad commercial scale** via the service catalogue of the provider.

It can thus be assumed that the second condition “not at a broad commercial scale” will only be relevant in few cases when the first-mentioned condition “the majority of main features are tailored to the needs of an individual customer or all components have been developed for an individual customer” is met.

c) Which criteria can be drawn on for classification as “tailored” within the meaning of Article 31(1) of the Data Act or “for testing and evaluation purposes” within the meaning of Article 31(2) of the Data Act (eg duration of testing/evaluation phase or whether the service is provided free of charge)?

A data processing service is “**tailored to the needs of an individual customer**” if the functional configuration of the service is specifically geared to the technical,

organisational or legal requirements of an individual customer. This is not merely a question of the parametrisation of a standard product but entails a substantial adjustment or development of the core functional logic.

Such tailoring can be assumed in particular in the following examples:

- Development of customer-specific data models
- Implementation of individual analysis algorithms
- Adjustment of the workflow or pipeline logic to internal business processes
- Development of special AI models based on internal company data

For example, a data processing service could be developed especially for the production control of an industrial enterprise that processes sensor data from specific machine formats and applies company-specific optimisation algorithms. In this case the main features of the system would be tailored to the specific operating procedures of this company.

By contrast, there is no tailoring to the needs of an individual customer if only:

- configuration parameters are changed,
- standard modules are activated or deactivated,
- user interfaces are adjusted or
- general integration takes place via standardised APIs.

In these cases the underlying functional architecture of the service remains unchanged.

The Digital Omnibus package will address this provision and if necessary reform it in future. While the English language version currently refers here to “custom-built” solutions, the new approach aims to govern “custom-made” solutions. The Staff Working Document understands “custom-made” as referring to data processing services for which the majority of features and functionalities have been **adjusted** by the provider to the specific **needs of the customer**.[107] While **“custom-built”** places the focus on the technical development process by which a solution (or its main functionalities) is **newly developed** specifically for a given customer, **“custom-made”** is more broadly defined and also includes solutions that are based on existing modules but have been **adjusted to individual requirements**.[108]

However, legal uncertainty arises from the correspondingly amended German language version. Specifically, the draft of a new Article 31(1a) of the Data Act speaks of “data processing services where the majority of features and functionalities of the data

107 See Commission Staff Working Document, 19 November 2025, SWD(2025) 836 final, page 24.
108 See Commission Staff Working Document, 19 November 2025, SWD(2025) 836 final, page 24.

processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025". The addition of the term "features", which was not previously contained in the legal wording, could mean that secondary features are also included in the provision's scope of application in the future. Until now, the wording has merely referred to "the majority of main features".

However, the EU's English language clarification supports the interpretation presented here according to which the adjustment of existing modules will already be covered by this exception. The reason for this deliberation on reform is that unlike standard solutions (off-the-shelf), contracts for the provision of such services are normally the outcome of targeted negotiations. If such contracts were concluded prior to the entry into force of the Data Act, expensive renegotiations may be necessary for these products to bring them in line with the provisions on cloud switching.[109] The EU intends this specification to save providers the corresponding costs and associated administrative outlay as it did not wish to include this form of services under the provisions on cloud switching.

The expression "**provided for testing and evaluation purposes**" describes the temporary provision of a service for testing or evaluation purposes, eg as part of pilot projects or demonstrations.

Such provision can be assumed, for example, in the case of:

- test versions (trial) with a limited scope of functions
- pilot runs (proof of concept)
- demonstration environments (demo system)
- time-limited access for evaluation purposes

In these cases the service is not offered as a fully productive service but is intended to enable the customer to assess its technical performance. The exception therefore does not apply to "data processing services that already exist as a full version and for which a functionally reduced test version is provided merely for reasons of customer acquisition (**trial versions**)."[110]

No explicitly specified individual factors can be derived from the wording for classification as "for testing and evaluation purposes" within the meaning of Art. 31(2) of the Data Act; a **teleological and systematic interpretation** is therefore decisive.

The following criteria in particular speak in favour of a test or evaluation version:

---

109 See Commission Staff Working Document, 19 November 2025, SWD(2025) 836 final, page 24.

110 Specht/Hennemann/Linardatos, DA/DGA, second edition, Art. 31 side note 15 with reference to Lienemann in Hennemann et al., Data Act p. 185; forthcoming also BeckOK DatenschutzR/Schmidt-Wudy DA Art. 31 side note 21.

- **time limit** of availability for use (the shorter the duration of availability for use, the higher the likelihood of provision for testing or evaluation purposes. The service must have been **configured from the outset for a limited time period** (eg test phase, trial, pilot). Unlimited or in effect permanently renewable use speaks against a testing purpose.)
- **limited functional scope**, ie reduced scaling or performance or use of synthetic data or test data (**a reduced or restricted version** (eg limited features, restricted data volume, restricted user numbers and performance) that differs from the full version is usual. In particular, no (permanent) data migration takes place.)
- **contractual arrangement** (contracts / GTC **explicitly** mention the **test character** (eg “evaluation license”, “trial agreement”), including term, intended use and exclusion of productive use.)
- **facilitation of functional or suitability tests** / lack of integration into productive systems (provisioning is intended to serve the customer **primarily for assessment, testing or evaluation purposes** (including functional or suitability tests), but not for productive use in operative business.)

Example: the service provider grants a company access to a demo instance of a data analysis platform for a few weeks so that this company can assess whether the service is suitable for its requirements.

The fact that this is free of charge does not constitute a separate criterion in this connection but can be drawn on as a factor for the overall assessment. **Provision free of charge** is a strong indication of a testing purpose but **not imperative**. Pilot phases subject to charge can also fall under Article 31(2) of the Data Act if the evaluation purpose is paramount.

The decisive factor is the **overall evaluation**, whereby the **time limit and evaluation purpose** are the core criteria. If a genuine test version is merely provided with restricted functionalities by the service provider and no integration into the customer’s system is carried out (or only test data are used), it is likely in practice that there will also be no need to switch service provider, so that this case is probably of subordinate regulatory relevance.

6 Conclusion

This study focused particularly on the question of how the identification of the same service type of data processing services can be operationalised in practice. Identification of the same service type is ultimately decisive for determining whether the entitlements set out in Chapter VI of the Data Act apply when switching provider.

A suitable multilayer classification model was therefore developed especially for determination of the same service type (see section 3). To our knowledge, this is the first comprehensive attempt in scientific literature to carry out a systematic classification of the same service type in accordance with the Data Act definition. The classification model set out was subsequently subjected to a practical test by classifying the services of relevant providers of cloud services on the basis of the classification model. The high share of the providers' cloud services assignable on the basis of the model indicates the fundamental suitability of the model.

Table 6-1: Illustration of the structure of the classification model in section 3

Dienstmodell	Haupt-ziel	Hauptfunktion	Level-0	Level-1	Level-2	Spezifikation der Abgrenzung/Portabilität (Was macht die Hauptfunktion einzigartig?)	Illustration
IaaS	PD	Virtual Infrastructure	Compute	Virtual Infrastructure	Virtual Machine Hosting	Virtual CPU/RAM/OS interface	EC2 / Azure VMs / Compute Engine
			Compute				EC2 Bare Metal / Bare Metal Instances / Bare Metal So-
			Compute				
PaaS	PD	Managed Orchestration	Compute				rvices
			Compute	Managed Orchestration	Serverless Containers	Container Resource Spec	AWS Fargate, Google Cloud Run, Azure Container Apps
			Compute	Managed Orchestration	Function-as-a-Service (FaaS)	Function code and / or runtime API	Cloud functions such as Lambda
			Compute	Specialized Compute	Quantum Processors	Quantum circuit interface	Braket / Azure Quantum

see section 3.2.5 for the full classification model

At the same time, the complexity of the model with its requisite sub-levels and the outlined discussions of possible borderline cases reflects the difficulties entailed by the definition contained in the Data Act for determining the same service type. This complexity makes it harder not just for the regulator, but also for the companies on the market to conduct a rapid and reliable assessment of whether claims from the Data Act with regard to cloud switching arise in a specific case due to the presence of the same service type. Not least for this reason, the cloud providers and customers interviewed in this study appear sceptical about the expected practical effect of the rules contained in the Data Act on switching provider.

It will be necessary here to monitor and analyse precisely which effects actually arise in practice when switching provider due to the Data Act. Should the observed developments not have the intended effect on the market, there will be a need to consider whether any adjustments to the existing provisions in Chapter VI of the Data Act are necessary. For example, one potential option to consider would be to simplify the definition of the same service type and conversely to exclude the SaaS layer from the scope of application of Chapter VI of the Data Act as it is precisely at the SaaS layer that the same service type is most difficult to determine. Concentrating on IaaS and if applicable PaaS while simultaneously simplifying application of the provisions from Chapter VI of the Data Act would make it more difficult for the providers at these levels to evade the obligations of

the Data Act. At the same time, these levels are the most concentrated in terms of market power so that the greatest need for action also exists here.