

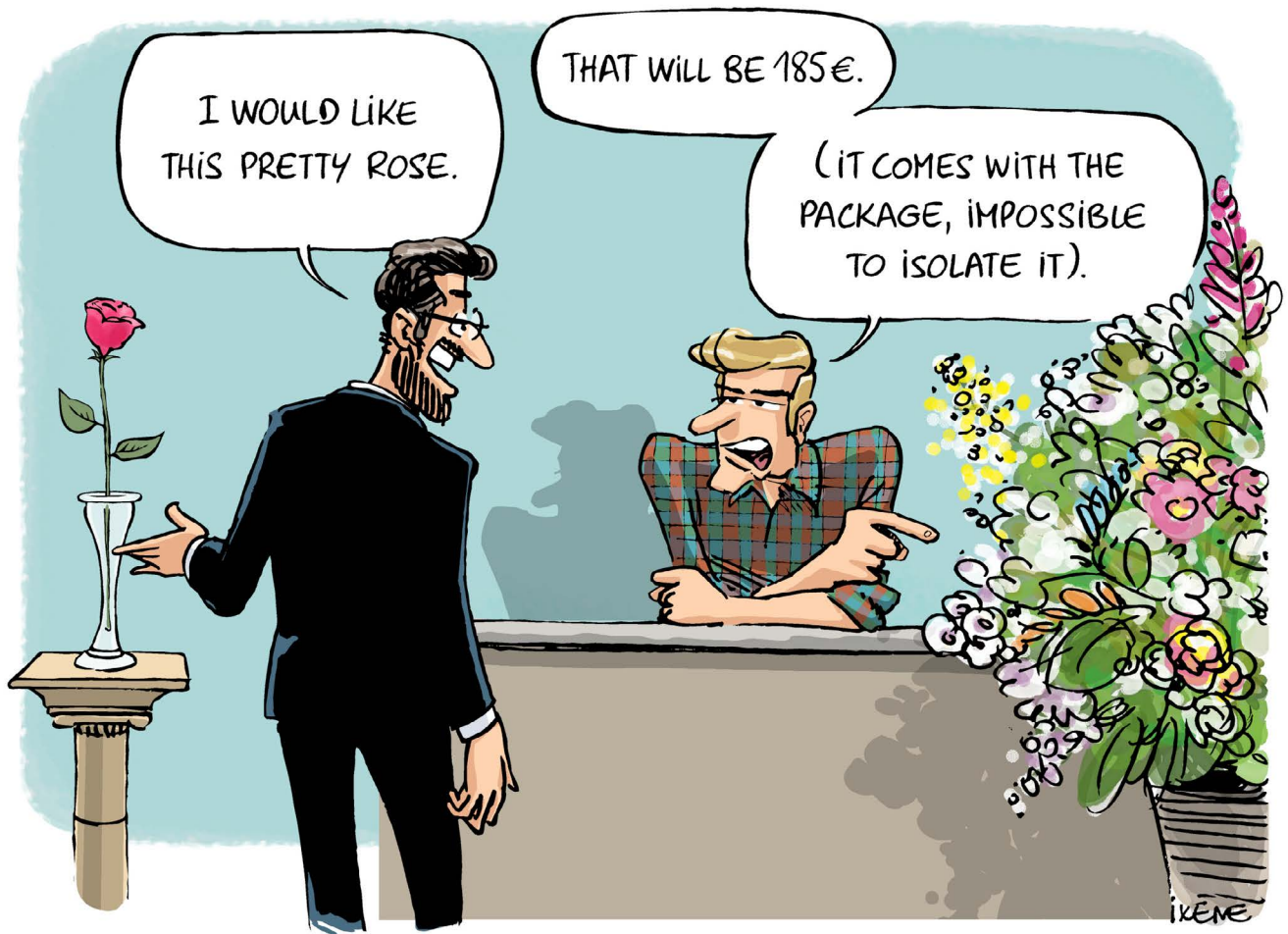


# 11 fair principles

## To unleash the digital potential of Europe

Business users' associations call for a balanced cloud market

November 2025



# Table of contents

<b>Principle 1</b> .....	<b>9</b>
The vendor shall fulfil existing regulatory obligations.	
<b>Principle 2</b> .....	<b>13</b>
Vendors must not create a technical or commercial lock-in.	
<b>Principle 3</b> .....	<b>17</b>
Customer shall remain in control of their own data and all the data uploaded or processed by the service/solution.	
<b>Principle 4</b> .....	<b>22</b>
Contractual terms and conditions shall be clear, unambiguous and not unilaterally changeable.	
<b>Principle 5</b> .....	<b>27</b>
Contractual terms shall not restrict or discriminate against the customer's choice of cloud provider, outsourcing partner or hardware platform.	
<b>Principle 6</b> .....	<b>31</b>
Contractual terms for licensing and subscriptions shall be free from geographic and entity restrictions.	
<b>Principle 7</b> .....	<b>35</b>
Contractual terms shall allow customers to use progressive or innovative technologies and deployment models.	
<b>Principle 8</b> .....	<b>41</b>
Service levels and product specifications shall be explicitly listed and take into account the customer's context.	
<b>Principle 9</b> .....	<b>45</b>
Commercial models shall not be changed unilaterally and shall adhere to an active 'opt-in' principle.	
<b>Principle 10</b> .....	<b>49</b>
Commercial models and offerings shall be consistent and reasonable, not combining different models for the benefit of the vendor's revenue.	
<b>Principle 11</b> .....	<b>53</b>
The scope, execution and intended outcome of an audit shall be clearly defined in the contract.	

# — Editorial

## Companies, hospitals, public institutions, universities and other European organizations deserve a better cloud environment.

Many organizations depend heavily on their cloud solutions. However, the imbalanced relationships between cloud providers and their business customers lead to unfair practices. European regulations offer several possibilities to improve the situation. Based on concrete examples of harmful practices on the market, our four associations propose 11 fair principles in B2B relationships between business users and their cloud providers, to lead the European and national legislators. This document can also be used by user organizations and suppliers wishing to demonstrate responsible practices.



One of the major promises of cloud is transparency and simplicity. Budgeting is said to be easy. However, the reality is quite different.

- *Emmanuel Sardet, President of Cigref*

### A non-competitive environment requires fair principles

The cloud market is characterized by several features that are unfavorable to business users:

- Once software is implemented, it is strongly entwined with the business processes. There is **vendor lock-in: switching to another provider is so complex and costly** that organizations are often effectively bound to their supplier.
- Business users **do not have bargaining power** vis-à-vis the large software suppliers.
- Cloud providers can unilaterally change subscription prices and the metrics on which the prices are based. Organizations cannot build a business case if they cannot predict future costs.



A company using ticket machines paid a fixed price/month/machine for the software. After some time, the software vendor changed the model to subscriptions based on the number of people using the machines. Not only did the vendor's decision completely change the business case, it was also very complex for the company to get organized, as the machines are being used in different application environments.

- *Hans-Joachim Popp, Deputy chairman of VOICE*

- In addition to large software and cloud providers, niche players can also have a dominant position vis-à-vis their customers, due to the dependence of the customer on the software or cloud service provided.
- There is **market concentration and dominance** by a couple of large players for a significant part of the cloud business market. Strong software providers copy features from smaller competitors and integrate them into their software. This **reduces both competition and customers' choices** and thus increases their dependence.
- There is a huge appetite for data to train artificial intelligence (AI). As customers entrust their data to cloud providers, business users are expressing concerns that the providers may train AI models on this company data.



When considering a provider, prices are dropped and features are promised. After signing, hidden costs emerge and features do not come as promised.

- *Martijn Koning, President of CIO Platform Nederland*

- There is a tendency to **combine vertical offerings**. Software providers can limit the choice of infrastructure that business customers are entitled to use to run their cloud applications.
- The **costs and complexity for the business user to get their data back** from the provider at the end of the contract can be very unreasonable.



The cloud market is very heterogeneous. We aren't targeting specific cloud providers. The fair principles described should be respected by all cloud suppliers.

- *Claude Rapoport, President of Beltug*

## NOW is the time to act

In addition to the above-mentioned cloud-specific concerns, rising geopolitical tensions also make it essential for organizations to be able to mitigate the risks of dependence on non-European cloud providers.

The Digital Markets Act, Artificial Intelligence Act, Data Act (with Standard Contractual Clauses) and upcoming Cloud and AI implementation Act create opportunities to improve the position of European business users of cloud services vis-à-vis their service providers. However, they do not, in themselves, provide a complete solution.

**We call on the European Commission, the European Parliament, national governments and European and national regulatory and competition authorities to secure the future of the cloud in Europe. European organizations rely on cloud providers to achieve their digital transformation and deliver their services: it is critical that these cloud providers respect the rules of fair trade and healthy competition in the European market, so that all players can benefit from the opportunities.**

We invite all these bodies to:

- stop the **abuse of vendor lock-in and unfair practices** by cloud providers and ensure fair market practice in the digital technology markets
- promote balanced and competitive offers in the cloud market
- ensure that **control over data remains with the business users of digital technologies**, without incurring additional costs or other negative effects.



Some 30 years ago, the EU broke up the telecom operator monopolies, because Europe saw that competition in the telecom market would create many opportunities. Now, companies face lock-in at a much higher level on the cloud services market.

- *Danielle Jacobs, CEO of Beltug*

### Digital Markets Act (DMA)

The four associations are very disappointed that none of the large cloud providers in the B2B market were designated as gatekeepers for cloud services in the initial round of designations in September 2023. Several large cloud providers have a dominant position for cloud services and can abuse this position of power. However, in the Digital Markets Act (DMA) they do not meet the threshold for cloud services gatekeeper because these thresholds were set up for the consumer market.

We ask the European Commission to designate very large cloud providers in the B2B market, pursuant to Article 3(8) of the DMA. If these large cloud providers do not meet the threshold for number of users, the definition of 'users' must be reinterpreted. It is clear to anyone with knowledge of the cloud market that all users of cloud services – consumers and business users alike – are highly dependent on these services and their providers. Just like consumers, business users should be able to count on fair practices and active protection against abusive behavior.

Moreover, cloud providers operate marketplaces where they offer software, applications, services and pre-trained machine-learning models, including from third-party vendors. This means that cloud providers act as gatekeepers between the third-party software providers and the users. It is therefore both useful and necessary to apply the obligations set out in Articles 5 to 7 of the DMA to cloud marketplaces.

### The Data Act

The Data Act, which became applicable on 12 September 2025, includes several provisions that aim at improving the position of customers of cloud providers vis-à-vis their cloud service provider.

*The implementation and enforcement of effective switching is more essential than ever and has been thoroughly analyzed and discussed.*

In 2022, the European Commission set up a 17-person Expert Group to assist in the development of Standard Contractual Clauses (SCCs) in line with Chapter VI of the Data Act, as well as Model Contractual Terms for data sharing. The four associations nominated an expert to participate in the Expert Group.

From September 2022 to March 2025, the Expert Group held 19 official meetings chaired by the Commission services that acted as the group's secretariat. In between these official meetings, the experts worked in smaller drafting groups for each clause, which were then discussed during the plenary meetings.

Based on the work of the Expert Group, **the European Commission has published** non-binding Model Contractual Terms on data access and use and Standard Contractual Clauses for cloud computing contracts.

The Data Act also includes obligations for providers to eliminate switching costs as of January 2027.

Furthermore, it is important for companies to be able to mitigate the risk of dependence on non-European cloud providers, and essential for organizations that are required under the DORA regulation to have an exit strategy to ensure their resilience.

## About us – Who we are

We are the Belgian, Dutch, French and German CIO associations; communities of Chief Information Officers (CIOs) and other senior leaders who are responsible for digital technologies and digital transformations within private or public organisations. These are all business users of digital technologies. We do not represent ICT suppliers and consultants.

 **Beltug**

Beltug - Belgium

**Cigref**  
SUCCEED  
WITH DIGITAL

Cigref - France

 **PLATFORM  
NEDERLAND**

CIO Platform - The Netherlands

**VOICE**  
Bundesverband der  
IT-Anwender e.V.

VOICE - Germany

# 01

---

## **Principle 1**

The vendor shall fulfill existing regulatory obligations.

# THE VENDOR SHALL FULFILL EXISTING REGULATORY OBLIGATIONS.

## Description

Today, the local Data Protection Authorities enforce the GDPR process and monitor compliance. It is regrettable that in 2025 some providers still do not respect the GDPR framework. Therefore, the question remains: will they respect and apply new EU regulations such as the Digital Services Act (DSA), Digital Markets Act (DMA), Artificial Intelligence Act and Data Act, to ensure that Europe can continue to innovate and stay competitive in this global market?

Given the provisions of the US CLOUD Act, it is increasingly unlikely that US-based providers will be able to comply with EU regulations without violating the laws of their home country.

In addition, the rapid adoption of AI in business software is raising many questions about compliance.

Vendors that work in a certain industry, geography or regulatory environment shall comply with applicable regulations. Vendors shall take responsibility for the data they manage on behalf of the customer.

Furthermore, they shall provide cloud technologies in such a way that the customer can comply with the regulations to which they are subject.

When regulatory frameworks evolve, vendors shall adapt or make available the necessary options to enable their customers to fulfill their regulatory obligations and remain compliant.

When a vendor cannot comply with (part of) a regulatory obligation, it shall inform its customers, allowing these customers to assess their own compliance and giving them the opportunity to either implement controls on their side or stop the contract.

## Examples

Under the GDPR, protection of personal data is to be guaranteed by all parties involved in the processing of these personal data.

Vendors must fulfill their duties as Processor and/or Controller, adhere to contractually agreed location of data processing (including hosting or remote support), etc.

While vendors might perceive the services they offer in the cloud as 'location-independent', when providing such services to customers subject to the GDPR, the vendors must fully comply with the GDPR, including its data transfer obligations. Vendors shall adapt their offerings in order to be compliant. We know of several cloud providers that, through Data Protection Impact Assessments (DPIA) or GDPR supervisory authorities, have been found not in compliance with the GDPR.

Similarly, under the Data Act, companies offering services in the EU or processing data generated in the EU must comply with the regulation. However, although the Data Act applies, the model clauses under it are not mandatory, while the Standard Contractual Clauses (SCCs) under the GDPR are.

The AI Act also introduces obligations regarding transparency, risk classification and accountability in AI systems. Vendors must proactively adapt their services *and inform their clients* in order to meet the evolving regulatory requirements. Authorities should proactively challenge vendors to verify this, as vendor negligence is detrimental to the rights of their European clients.



**“ No one is above the law. Big or small, European or non-European, software company or cloud provider ... if you want to do business in the European data economy you must follow the EU rules. Every vendor shall fulfill existing regulatory obligations. And shall do it now. No excuses.**

**”**

# 02

---

## **Principle 2**

Vendors must not create a technical or commercial lock-in.

# VENDORS MUST NOT CREATE A TECHNICAL OR COMMERCIAL LOCK-IN.

## Description

There are several forms of lock-in:

- Technical lock-in: arising from the application of specific technical environments or proprietary formats that result in significant redevelopment or high migration costs.
- Commercial lock-in: arising from specific licensing practices or conditions, such as low or even free first-year offers or new pricing models that result in future cost of ownership beyond the customer's control. Loyalty discounts and rebates are frequently linked to predatory pricing and bundling. They make it difficult for customers to assess the value of a product or service, as well as the actual advantage granted by the supplier. In the medium-term, price discounts offer a financial advantage. In the long-term, however, they lead to an extension of the supplier base and an increase in the customer's dependence. There is also the risk of losing this advantage when the contract is renewed or if the vendor is acquired by another company.

Software vendors shall adhere to open technical standards wherever such industry standard exists. Customers shall not be intentionally restricted in any commercial or technical way from exercising their right to port their data between vendors, switch providers, or regain access to their own data. Interoperability between non-proprietary or comparable technologies shall be technically supported.

Inter-cloud data transfer shall be possible, allowing business users to shift data at will between cloud providers for processing.

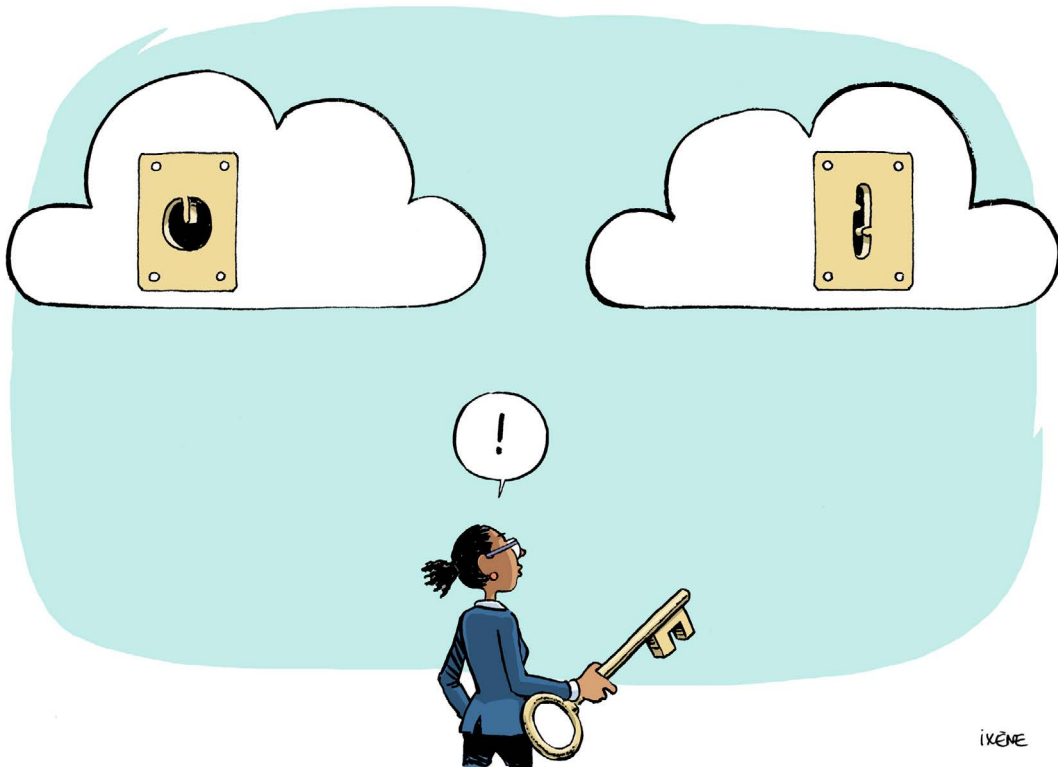
In order to enable switching, data shall be handed over in a non-proprietary form such as .txt or .csv or a human-readable format. It shall be clear what type of information it contains: database back-up, images, words, figures, drawings, etc.

This principle is recognized in the Data Act.

## Examples

- When business customers want to change vendor and request the return of their own data, they receive that data in a format linked to the vendor. Although the customer has technically recovered their data, in practice the data is only accessible through the use of a format that is the property of the vendor. As a result, the customer remains dependent on the former vendor even after contract termination, enabling the vendor to continue to impose restrictions, increase costs, and cause delays.
- Open standards for virtual workload in the cloud do exist, but the standards have not yet been adopted nor uniformly applied. Wherever such a standard exists, vendors shall apply it, so that switching is possible. Without endorsing the specific standard, one example is Cloud Foundry for container workloads.

- Providers sometimes introduce contractual clauses and technical barriers that hinder data portability and interoperability. These restrictions deprive customers of one of the essential benefits of the cloud: flexibility. Within the same solution or application portfolio, vendors may restrict the release of new functionalities or cease support altogether for customers that fail to adopt the latest technology stack. Consequently, customers are compelled to migrate from cost-effective, self-hosted on-premise solutions to public cloud in order to secure and receive timely updates, access to future releases and the product roadmap. However, this transition increases the risk of technical and commercial lock-in.
- In the current geopolitical situation, this heightened dependence due to lock-in is unwelcome, and puts European business users at even greater risk. New features may, for instance, undermine the customer's control over their own data and services, or add functionality that is not needed but drives up costs, impacting the competitiveness of the European customer's own products and services. The control of the provider over its cloud service means these changes can be introduced with every update.
- As a consequence of lock-in, customers often make unproductive software deployment decisions to avoid increased fees. Since the option to change vendors has become uneconomical, customers may stay on legacy or unsupported platforms, creating additional operational risk, as migrating to a newer or different environment would require unjustifiable software investment.



**“ Since September 2025, the Data Act has been a reality.**

***Business users expect their providers to comply with the obligations.***

**”**

# 03

---

## **Principle 3**

The customer shall remain in control of their own data and all the data uploaded or processed by the service/solution.

# THE CUSTOMER SHALL REMAIN IN CONTROL OF THEIR OWN DATA AND ALL THE DATA UPLOADED OR PROCESSED BY THE SERVICE/ SOLUTION.

## Description

Privacy is a basic human right and the GDPR framework ensures (by introducing the explicit consent principle, among other things) that personal data must be handled correctly. But what about company data?

All too often, vendors consider the customer's use of a service as consent to allow the vendor to process and use the customer's data for purposes outside the delivery of the service.

The standard terms and conditions shall specify the customer's right to their data, the processing and the restrictions. Data that has been processed and potentially enriched by the vendor's solution and relevant metadata shall remain the sole property of the customer. The proprietary algorithms shall remain under the ownership of the vendor.

Vendors shall not reuse data from the customer for their own purposes (such as service improvement or statistics).

Data is both input and output for cloud providers, who create value through a data transformation process in which some providers become even more powerful. Once data is hosted by the provider, several crucial questions arise:

- How can the customer access or retrieve the data, how often, and at what cost?
- What does the provider do with the (consolidated) data?
- Is the cloud provider using the customer's company data to train their AI models?

Companies are worried that:

1. cloud providers may apply contractual clauses ambiguously to permit the use of customer data for training AI models.
2. cloud providers will not respect the contract or will grant themselves the right to use the data in a non-contractual way, by omitting explicit statements.
3. they lack the expertise to assess contractual risk, exposure, etc. For example, how can companies stay more vigilant than a cloud provider?

With the growing use of artificial intelligence (AI) in cloud solutions, vendors benefit from broad user bases, often coming from a specific industry or domain of interest of the vendor. As customers upload data and use the solution, they unknowingly contribute their data to training and optimizing the vendor's AI model. In a cloud context, and especially in a multi-tenant setup, the model is controlled by the vendor and fed by many clients. Vendor contracts often stipulate that the original data uploaded by the client remains the customer's property, but the trained AI model — and in some cases the resulting data outputs — are considered the vendor's intellectual property. Not only do the customers lose ownership of the trained model and potentially sensitive or competitive knowledge, they also find it difficult to migrate away from the vendor while retaining the trained model that is in a proprietary format.

It has been observed that many vendors give away free trials, which are appealing to technical staff who want to explore the boundaries of technological progress. However, even in trial scenarios, vendors create trial agreements that assign ownership to themselves.

### Unbalanced liability terms

At first glance, both the provider and the customer are liable for breaches of confidentiality: the provider needs to ensure the confidentiality of the data that the customer stores with them, while the customer needs to maintain the confidentiality of the contract itself.

Concerningly, the current liability terms in cloud service contracts are heavily unbalanced. Clients bear unlimited liability for breaches of confidentiality, whereas the providers' liability is capped at the value of the annual service fee. In other words, while a breach of confidentiality by the client can have far-reaching consequences due to substantial claims from the provider, the provider faces only a limited penalty even if it acts in bad faith; for instance, selling the client's data to one of its competitors. This imbalance in liability unfairly favors the service providers at the expense of the business users.

### Use of data by the provider

Vendors shall specifically state that they cannot, do not and will not use customer data, data generated by the customer, or data derived from the customer's use of its data in any way, unless this is transparently and contractually agreed to by the customer and the customer receives due compensation.

## Examples

There are multiple examples of vendors deeming a customer's use of a service as consent to process and use the customer's data beyond the delivery of the service. For instance:

- Platform for managing customer's stock options: the data to make the calculations comes from the customer while the calculation method comes from the platform. However, the platform claims that the new data generated, i.e. the calculations, is its property.
- Data mining service: the service operates solely on the customer's data, but the vendor deems that the output of the process is its own property, which it may sell to other companies. The algorithms are owned by the data mining service, and the customer pays for implementation. However, the insight and improvements gained through optimizing the customer's processes are presented as best practices and offered to competitors of the customer.

In contrast, here is a positive example illustrating how customers can remain in control of their data through clear contractual terms and conditions:

- A software provider developed an application offering the functionalities required by insurance brokers to manage their business. The SaaS contract between the software provider and each broker is clear:

*“The software provider will host on its servers – or those of a cloud provider – all the data of the insurance broker ... The data of the insurance broker hosted on the software provider servers – or those of a cloud provider – REMAIN FULL PROPERTY of the insurance broker.”*

In this example, the software provider explicitly guarantees that neither it nor its suppliers will access or use the data except as described in the contract and the law. The software provider thus engages to guarantee the confidentiality of the data to which it has access. Each insurance broker using the software remains full owner of its respective data; there are as many separate databases as there are brokers using the software, and each broker decides to which user it gives access.



“ *The GDPR framework ensures that personal data must be handled correctly, but what about company data?*

*Organizations are worried that the cloud provider will train its AI models on their data.*

”

# 04

---

## **Principle 4**

Contractual terms and conditions shall be clear, unambiguous and not unilaterally changeable.

# CONTRACTUAL TERMS AND CONDITIONS SHALL BE CLEAR, UNAMBIGUOUS AND NOT UNILATERALLY CHANGEABLE.

## Description

The terms and conditions proposed by providers are complex, multi-page legal documents that lack simplicity, use words open to interpretation, and are usually very unilateral. They stand in stark contrast to the user-friendliness and simplicity of the respective software and cloud solutions.

### Clear and unambiguous

Organizations conclude contracts with various vendors, but there is no consistency in contract terms between them. The same metric can be defined and calculated in very different ways across vendors.

Contractual terms shall be written and agreed in generally understandable and unambiguous language. Definitions shall be clear and concise such that the signing parties are able to determine their obligations. Capitalized terms shall refer to an explicit definition in the agreement. Uncapitalized terms shall refer to a generic, non-proprietary use of the word in common language.

In terms of usage perimeters, IT license contracts shall clearly define permitted uses, with any use not expressly authorized by the rights holder prohibited. Particular attention shall be given to clauses on license transfers, indirect access and user definitions, which often vary and can create compliance risks, especially in hybrid or reorganizing environments. Lack of contractual flexibility can hinder adaptation to evolving organizational structures and access models.

### Minimum terms and conditions

The terms and conditions shall cover at least: metric definitions, solution and service descriptions, restrictions, terms and termination rights (including exit clauses), data ownership including residency, intellectual property provisions, anniversary and renewal notifications, balanced liability, responsibilities and restrictions.

In case terms and conditions are not explicitly included in a signed agreement, the terms and conditions at the time of signature shall apply. The vendor shall not apply different terms and conditions to a contract that has been agreed prior. The vendor shall ensure the customer has access, either publicly or upon request, to the terms and conditions that apply from the time of signature. The vendor shall make available at least the following information for the customer's contract management: name changes, support lifecycle and price lists.

### Not unilaterally changeable

There is a reason why terms and conditions are negotiated: once written and agreed they are fixed in the applicable contract, terms of purchase and any annex. The terms and conditions may be set out in a master agreement, framework agreement, license agreement or any downstream order form or purchase document referring to the main agreement structure.

The practice of referencing terms and conditions through a website or online location (URL) must be explicitly agreed by both parties, as the customer cannot control unilateral changes or updates to the terms and conditions made by the provider. URLs are often recursive: online general terms and conditions may refer to other URLs for service level agreements, data processing agreements, product specifications, etc. This approach is very common for cloud contracts, most of which include a reference document (the 'framework agreement') to which other contractual resources are attached. However, if these resources are available on a website, they may be changed by the vendor over time. Therefore, it is essential for customers to require advance notice of any changes.

In order of precedence, customers expect:

1. Reviewed and signed static documents that cannot be unilaterally changed.
2. Advance notice subject to written agreement between the parties.
3. Advance notice with a sufficiently long notice period to allow for the remediation of any risks.

Vendors may be permitted to make changes to the language of the agreement provided that these changes have no material or financial adverse effect on the contracting organization (e.g. the customer) and that the customer is notified in advance and given the opportunity to review and reject such changes.

### Strategic autonomy

The terms and conditions shall explicitly outline the applicable law governing the access to the processed data. Vendors must permit data localization based on the types of data being stored and comply with client-imposed restrictions (e.g. health, financial or government data). Additionally, clients shall ensure that no other laws or legislations allow foreign governments or companies to access sensitive data without the client's explicit consent or judicial grounds in the law of the territory where the data is located. Vendors shall strictly adhere to client-imposed conditions regarding cloud and infrastructure sovereignty, ensuring that cloud services are operated under local jurisdiction or by customer-selected national providers.

## Examples

### 'Use' vs 'use'

The uncapitalized term 'use' refers to the common definition of putting something, such as a tool, skill or building, to a particular purpose. The customer has a benefit of a certain asset or service from the vendor. The capitalized word 'Use' may refer to a verb or definition with a broader meaning than 'use'. For example, 'Use' can denote the ability to use a service or software, or the availability of a certain capacity that has not previously been put to the benefit of the customer.

Typical wording that extends the definition of use beyond what is reasonable accepted and thus should be capitalized: "[use] every device that has the capability to execute the program". In this case, even not used, but with the capacity, it is counted..."

The change towards the possibility that something is used was included intentionally. A customer that gave the possibility of several administrators to access a server, for example for reasons of ensuring continuity when the responsible administrator would be impaired, had to pay for that possibility, even when the customer could prove that only one administrator had accessed the server.

Typically and intentionally listing possible scenarios to make the definition of the common understanding of use broad, and redefining it as 'Use': "[use] Customer's installations, deployment, access of or provision of access to, or use of each Product". Agreeing to the definition of 'use' in this case has a negative effect on the calculation of fees. Provisioning something in this case leads to higher-than-expected fees. For a specific vendor, it seems the business model is based on making terms unclear, with the result that customers are charged more than the customers expected. Through a change of the definitions combined with an aggressive control and audit policy, the vendor put pressure on the just acquired customers to pay more.

### **Agreement to commercial documents leading to changes in terms and conditions**

When a contract requires extension, for example when a yearly subscription expires, vendors often include their latest terms and conditions by referencing the URL conditions in the renewal documents. Once the renewal documents are signed, the original, reviewed and agreed terms in the frame agreement that formed the basis of the initial contractual relationship are overridden and voided. As a result, the new terms and conditions, which have not been reviewed and agreed, may have a negative effect on the obligations of the customer under the initial, fully negotiated agreement.

### **Vendors cannot guarantee data localization and restrictions**

Vendors often offer local instances of single- or multi-tenant cloud solutions, ensuring that client data is not leaving the country or jurisdiction specified by the contract. However, they frequently collect and store metadata or derived information from global clients in a location outside the client-defined restrictions. Information such as performance statistics, login information, derived algorithms and AI models is often stored centrally with the vendor rather than within decentralized client environments. Contracts may lack details specifying what vendors may do with derived information. This lack of detail can then be exploited by the vendor to suit their own purposes.



“ The contracts proposed by providers are big legal documents, often more than 100 pages, with annexes, written to protect the provider and give them the power to evolve over time without the customer’s agreement. ”

# 05

## **Principle 5**

Contractual terms shall not restrict or discriminate against the customer's choice of cloud provider, outsourcing partner or hardware platform.

# CONTRACTUAL TERMS SHALL NOT RESTRICT OR DISCRIMINATE AGAINST THE CUSTOMER'S CHOICE OF CLOUD PROVIDER, OUTSOURCING PARTNER OR HARDWARE PLATFORM.

## Description

Customers that have purchased or are purchasing software shall be entitled to deploy and use it on the platform or with the cloud provider of their choice. The terms and conditions, including commercial terms, shall be non-discriminatory and uniform for comparable workloads and performance regardless of whether workloads are run in the cloud, on-premise or in any hybrid setup. When the technology and workloads are comparable and common, the customer shall have freedom of choice.

Customers shall not be at the mercy of the vendor for what they can use and shall be free to run a service elsewhere. Neither software vendor nor cloud provider shall limit or block this freedom of choice.

Cloud infrastructure has the same or comparable computing power and has the same limitations as on-premise workloads, with the sole exception that the underlying hardware is owned by a third party.

Customers who are moving on-premise workloads to cloud providers shall be entitled to a cost neutral migration that safeguards their investment for comparable performance and workload.

## Examples

### Various examples of restricted choice exist:

#### Bundling software and infrastructure

Many software vendors create self-maintained lists of authorized public, private or hybrid cloud infrastructures on which customers are entitled to use their purchased licenses. For instance, one major vendor prohibits the use of its software on the infrastructure of a major IaaS provider, while allowing two others under certain conditions. The list is subject to change and only contains a subset of common cloud providers in the industry. As the list is self-maintained by the vendor, customers run the risk that, in the future, the current infrastructure cloud provider can no longer be used.

This practice makes customers dependent on the vendor for what infrastructure they can use. Furthermore, cloud providers often bundle services and offer enormous rebates. While customers may be free to run a service elsewhere, they are uncertain of the future and forgo the rebates.

#### Limiting support for software when changing infrastructure cloud providers

Software vendors may also stop the support contract when the customer moves to a competitive cloud provider. The software vendors prohibit the usage of licenses on public cloud (IaaS) by restricting the use rights under the support agreement.

While the customer can choose to transfer the license to an IaaS environment, support is no longer included. So, even if the customer maintains an uninterrupted support stream, the eligibility for running the same licenses in an IaaS environment is at the sole decision of the software vendor itself, through the use of the support contract. One dominant IaaS provider only offers license mobility within its own products, unrelated to the IaaS service.

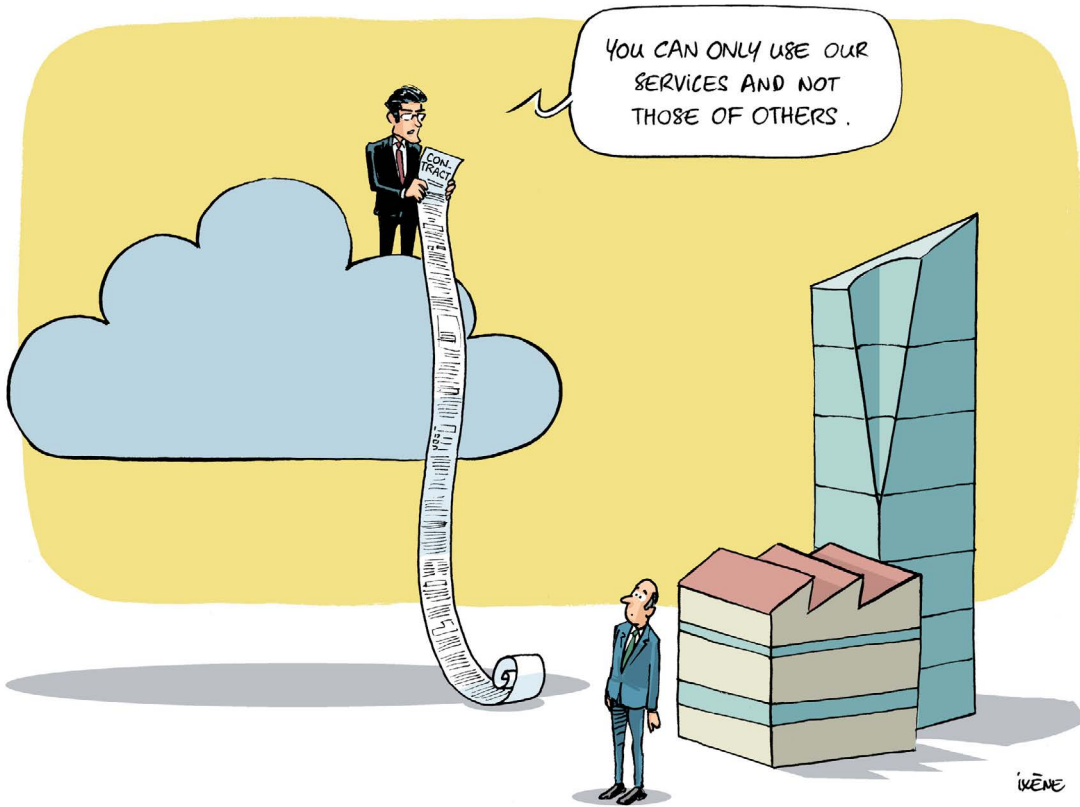
Another software vendor offers an incentive to run the customer's perpetual licenses on its IaaS cloud by giving more use rights per license when its IaaS cloud service is chosen.

A customer runs the software of a vendor on-premise, in its own data warehouse. For the use of the software, the customer has paid a license fee and pays a maintenance fee, a scheme which was and is standard. When moving to the cloud and looking for an IaaS provider, the vendor of the software allows for up to 90% conversion of the initial fees and all the maintenance of the software, when moving the vendor's software to the vendor's IaaS solution. If moving it to a competing IaaS solution, the customer would have to pay the full price. The benefit here is disproportionate and restricts freedom of choice.

### **Restriction of new software releases when SaaS is not fully adopted**

One major business software vendor openly states that customers using an on-premise version of the same code base will only receive critical updates (including security patches) and access to newly released features if they adopt the full SaaS model, rather than operating in a self-hosted environment or a hyperscaler environment.

This practice restricts the customer's choice for enabling the long-term viability of the use and productivity of the business software in favor of its own (private) cloud SaaS environment. Organizations have raised concerns that this practice may be contrary to the prohibition on abuse of dominant position under Article 102 TFEU, specifically on bundling. Moreover, migrating to the cloud effectively constitutes a point of no return, since switching back to on-premises hosting would incur significant costs and require considerable technical effort.



**“ Contractual terms shall not restrict or discriminate against the customer’s choice of cloud provider, outsourcing partner or hardware platform.**

- *Customers purchasing software shall be entitled to deploy and use the software on the platform or with the cloud provider of their choice.*
- *Customers who are moving on-premise workloads to cloud providers shall be entitled to a cost neutral migration that safeguards their investment for comparable performance and workloads.*
- *Customers shall not be at the mercy of the vendor for what they can use and shall be free to run a service elsewhere. Neither software vendor nor cloud provider shall limit or block this freedom of choice.*

**”**

# 06

---

## **Principle 6**

Contractual terms for licensing and subscriptions shall be free from geographic and entity restrictions.

# CONTRACTUAL TERMS FOR LICENSING AND SUBSCRIPTIONS SHALL BE FREE FROM GEOGRAPHIC AND ENTITY RESTRICTIONS.

## Description

The cloud has no borders, and Europe ensures free movement of goods, services, capital and people within a single, internal EU market. However, vendors in the business software and cloud services industry don't market their solutions with this open attitude and mindset.

While business software and cloud services are generally operational cross-border and are not tied to any legal entity context, the vendors of such solutions usually limit the perimeter of their licenses. When a customer changes their business or geographical perimeter, a new contract must be renegotiated, which creates a new opportunity for the vendor to modify the terms and conditions or to increase the price.

It's not the vendor's role to define the expected use and geographical area in which the business software and cloud service may be used. Customers are responsible for ensuring access is granted only to users within their enterprise and for deploying the solution in compliance with technical requirements. Accordingly, no restriction shall be imposed by the vendor regarding geography or legal entity. Commercial terms are rarely based on the physical location of the business users or the legal entity to which they belong, and the vendors are not adversely impacted by such metrics. The same applies for metrics based on compute power, capacity, storage, etc. The expansion of the organization or geography will impact the vendor's revenue in a transparent and logical manner.

## Examples

- In some cases, contractual terms explicitly restrict the software use to a single legal entity: *"Licensee' means (a) the company or other legal entity on behalf of which (name vendor) are acquired [...] For clarification, 'You' refers only to a single, specifically identified legal entity or individual, and does not include any subsidiary or affiliate of any such legal entity or individual or any other related person."*
- The terms may also restrict the entity to a specific licensee. The following example comes from a publicly available part of the contract terms of a major software provider and shall not hold, as it restricts the use of the license based on territory: *"We grant you a [...] license to deploy the Software within the Territory" and "Territory means the country or countries in which you have been invoiced, except as otherwise provided in the Product Guide. If the Territory for your Software includes any European Economic Area member states or the United Kingdom, you may deploy that Software throughout the European Economic Area and the United Kingdom."*
- In another case, global deployment rights can be unilaterally revoked by the supplier; the customer can only get them back by paying an amount into a 'fund' from which additional licenses can be purchased later (regardless of whether the user needs them or would like to purchase from the supplier).

- In still others, the license metric is defined as a specific 'site' or 'office' location. Global customers operating within matrix organizations may experience a detrimental effect on their software cost if a team member is suddenly using the same software in another 'site'. Permanently remote workers and digital nomads also do not fit these outdated license models.



“ Often the provider wants to limit the perimeter of the license. So if a customer increases its business or geographical perimeter, a new contract has to be renegotiated.

*Vendors shall not restrict usage to only the contracting entity and the customer shall have the flexibility to use the purchased subscriptions within the same enterprise, group of companies that form a holding or group of entities with the same objectives or otherwise connected. All current and future entities shall be covered, as long as they are majority-owned.*

”

# 07

---

## **Principle 7**

Contractual terms shall allow customers to use progressive or innovative technologies and deployment models.

# CONTRACTUAL TERMS SHALL ALLOW CUSTOMERS TO USE PROGRESSIVE OR INNOVATIVE TECHNOLOGIES AND DEPLOYMENT MODELS.

## Description

Software terms and conditions are always based on underlying technologies. But when the technologies progress faster than the software terms, it creates a disconnect between the usage, now based on the advanced technology, and those terms. The software terms still refer to an old concept of calculating the required entitlement, while the new technology has progressed to a different licensing concept.

Vendors use software terms and conditions in their favor if they can be interpreted in such a way that the customer needs to make incremental investments to cover the same functionality, while the technology enables better use.

Therefore, software terms shall, within a reasonable timeframe, adopt licensing rules that give the benefit of technological progress to the customer. More granular and efficient management of compute resources shall be recognized and supported by a vendor offering to run the software on such advanced technologies.

Customers note that the vendors are up to speed technically, and have embraced the new development. When they contact a vendor's support staff (for which the customers pay through maintenance contracts), the vendors are able to solve the issues. But, when the contracts are being discussed, the vendor ignores the technological change and works as if the software is still running in the previous environment.

Apart from increased efficiency and thus potentially less revenue for the vendor, new technologies also provide more certainty in terms of business continuity and a more agile organization. These are advantages that do not impact the vendor, but that do benefit the customer. In such cases, if the vendor applies the old framework, this leads to a more difficult business case or even to the customer not adopting the new technology.

## Examples

- Many vendors apply terms and conditions that force customers to license more cores when using virtualization, complicating the business cases. Some customers have agreed to install software that tracks the number of cores being used, which introduces an additional workflow for the customer.
- Furthermore, each vendor establishes its own rules and procedures, as well as different metrics depending on the type of core. Starting from the physical cores and extending through the types and versions of machines, all the rules are considered in order to determine the number of virtual cores that the customer must license. Even worse, in some cases, when a system arrives at the end of its supported life but the customer can't decommission it (for whatever reason), certain vendors revert to counting the system by its physical core, leading to unnecessary complexity.

- Finally, customers using advanced autonomous or agentic AI systems, such as robots, cannot be accurately quantified using traditional license metrics. The effective use and commercial valuation of software must evolve to reflect the distinct operational characteristics of neural networks and non-human agents, rather than relying on human-centric licensing models.

## **Below are some examples of software vendors' practices:**

1. One vendor begins by differentiating between on-premise and cloud for the license model. But, as technology has progressed, several other options have become available, including co-location, private cloud or managed datacenters. The question arises: do these newer options fall under the 'on-premise' or 'cloud' designation?

If considered as cloud, the licensing model includes an additional administrative fee payable by the customer, in order to be able to move the software (which the customer has already paid for) to the cloud. This is an extra and unfair burden (see principle 10). On top of the fee, the vendor reserves the right to review the licensing if the technology improves. This is a clear example of a vendor trying to capitalize on improvements it has not contributed to.

If considered on-premise, several variables come into play: virtual or physical, dynamic allocation or not, fixed partitioning or not, multithreading with a 0,5 factor, but not in virtual setting, only physical, etc.

2. Other vendors start by differentiating between physical and virtual capacity. For physical capacity, the calculations have two metrics, within which the customer has to take into account:
  - some 40 different multipliers depending on the processor name and model number, server model and number of sockets.
  - a matrix with different multipliers for the first thousands, the next thousands and so on for the resources licensed.

One vendor has imposed a whole range of conditions for its software used in virtual systems. If the customer doesn't comply with these, the virtualization isn't taken into consideration and only the physical capacity is counted. For example, if the customer has 1 virtual machine with 2 virtual cores, but is working on a larger cluster with 400 cores, it is the 400 cores physical capacity that will be counted. The conditions include:

- The vendor decides if the software may be used on a virtual machine.
- The vendor decides if the virtualization technology is eligible. The vendor has, for example, excluded older versions of virtualization technology, forcing customers to update the virtualization technology. In principle, however, the vendor's software has no link with the virtualization technology.
- Some systems are excluded, depending on the end-of-life decisions of other vendors, while the newest versions of certain systems are not yet eligible. Again, these systems have no relation with the vendor, but it is the vendor, through its licensing policy, that influences the uptake or not of certain systems.

- The vendor determines which processor technologies the customer must use. With a growing number of companies developing their own processors, this might create a major barrier for those companies and for technological evolution.
  - The vendor requires the installation of a specific measuring tool to verify the use on the customer side. In many instances, the software doesn't work very well, creating a possibly significant problem for the customer. If, over the course of several years, something goes wrong, the vendor might annul the virtualization, leading to the counting of the 400 cores instead of the 2, as given in the example in the beginning.
3. One of the clearest examples of how customers are prevented from benefitting from technological progress comes from a vendor that always determines licensing based on physical capacity, even if everything runs on virtual machines. As in other examples, this vendor imposes multipliers depending on the type of processor. When that requirement is imposed for the whole cluster, and even all related clusters, a license is needed, despite the fact that the software is not running on the cluster. Even if the customer installs a measuring tool and can prove through the logs that the software has not turned on any of the other cores, the vendor still imposes complete licensing of all the cores.

## Optimization of computer power by virtualization and the use of containers

**Processors:** Software terms often treat processor licenses as traditional, physical on-premise workload. As such, they ignore the technologies that create more advanced levels of virtualized workload. While customers and infrastructure providers have moved from physical to virtual compute power, and more recently to containers, software vendors have created ever-more complex license calculations to increase the required entitlements. A software license calculation can require multiplications and divisions of various new criteria, ultimately leading to an elevated license requirement.

Rather than ensuring that the benefits of technological progress are split between the users and the providers of the new technology, the software companies change their contractual terms to ensure that such benefits are more difficult to realize: more overhead, less certainty. In extreme cases, some customers set up isolated compute environments in order to fulfill the licensing requirements while benefitting from the technology; an approach that goes against best practices for disaster recovery and back-up. A processor definition in the current context is no longer a physical electronic circuitry that executes instructions, but often a virtual and shared unit of processing abstracted from the physical device or environment.

**Desktops:** Software terms refer to a 'desktop' or 'seat' as a traditional physical device that remains at the office; they thus don't correspond with the current way of working in the modern workplace. Mobile devices, multiple devices per user and virtual devices accessible from any location are all common practice today. Interpreting the traditional metric in the current environment, with virtualization, leads to very complex license calculations. Vendors try to reflect what the calculation would have been in a world without virtualization. One user accessing a virtual desktop can be counted as multiple installs, since there is no physical limitation on the individual's usage or location.

A concrete example of this is a machine with two cores, which requires licenses for those two cores. The organization then moves to a virtual environment in order to improve business continuity: a break-down of the machine would no longer lead to a stop in the available computing power. In this scenario, two cores are still needed, but they are now virtual. The vendor, however, continues to argue that licenses are needed for all physical cores — which in a server environment supporting the virtual machine would easily climb to hundreds of physical cores — even though at no single point in time would more than two cores be working.



“ *Software terms and conditions are always based on underlying technologies. But when the technologies progress faster than the software terms, it creates a disconnect between the usage, now based on the advanced technology, and the software terms.*

*Therefore, software terms shall, within a reasonable timeframe, adopt rules that give the benefit of technological progress to the customer.*

*Virtualization as an example:*

*Software terms often treat processor licenses as traditional, physical on-premise workload. But customers and infrastructure providers have moved from physical to virtual compute power, and more recently to containers.*

”

# 08

---

## **Principle 8**

Service levels and product specifications shall be explicitly listed and take into account the customer's context.

# SERVICE LEVELS AND PRODUCT SPECIFICATIONS SHALL BE EXPLICITLY LISTED AND TAKE INTO ACCOUNT THE CUSTOMER'S CONTEXT.

## Description

Software vendors offering cloud solutions shall ensure and explicitly list the responsibilities they assume regarding their services. With a cloud solution, the customer abstracts away the lower layers of the technology stack. For example, in a SaaS model, the customer doesn't have access to the physical infrastructure, the network or the storage, but instead consumes only the front-end application or website. The agreement shall specify service descriptions, service level KPIs, the consequences for not meeting the service levels (credits, termination rights, etc.), and the response and resolution times.

Vendors shall define maintenance windows and excluded downtime so customers can align their critical business processes with the provided service continuity.

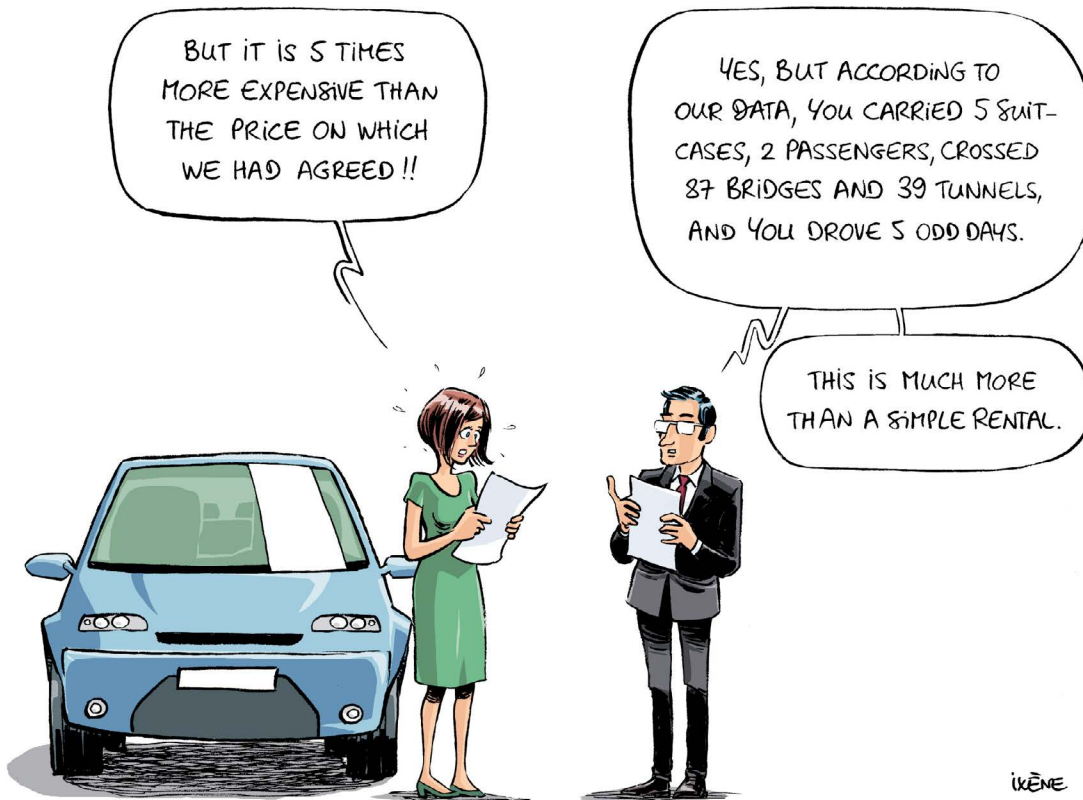
Vendors shall accept consequences that are proportionate to the impact of a failure and aligned with the criticality of the solution as well as the scope of the service for the customer. If the solution is critical for business continuity, the vendor shall not disclaim responsibility and shall offer a service that aligns with industry expectations.

This also applies to IP infringements, regulatory compliance and waivers. A SaaS solution can use both open and proprietary components, protected by IP. The vendor remains responsible for indemnifying and holding the customer harmless. In the case of waivers, the vendor shall also prove that it has taken all necessary measures to ensure regulatory compliance.

## Examples

- Software use is sometimes verified with license keys. One vendor initially used a separate server to verify the key. As the customer had their server on-premise, this 'extra' verification went smoothly. When the vendor moved the verification server to the cloud, due to the many integrations, the customer could not follow. This meant the verification could no longer be performed, and despite having a perpetual license for the software, it could no longer be used.
- Cloud providers often do not consider themselves business critical from an operational perspective and refuse to provide strong service level commitments. Nevertheless, they charge a premium fee for their services. As the services are in many cases business critical, organizations do contract them. One major cloud provider does not offer any service levels, making it impossible for customers to have a predictable environment to work in. When the services break down, there is no visibility on how long it will take before the service is restored.
- In other cases, maintenance windows are often not aligned with customer expectations, or upgrade cycles are too fast for customers to perform regression testing before the cloud upgrade is required (testing the impact of the upgrade on all processes and other software connected to the software that is upgraded). Some cloud providers release a new version twice a year.

For example, a small software solution generates serial numbers and writes these in the central ERP system. Without the software solution, the customer's entire production would stop. Therefore, the service level for this software solution needs to be high, as it is critical for the business. But the vendor doesn't offer a high service level, because in their opinion the software only fulfills a limited function in the production process.



“ *Cloud solutions are end-to-end solutions whose quality and availability must also be recorded. Clarity must be provided here through product specifications that are well-defined and interpreted in the same way by all parties. Availability must be detailed in a set of service levels that are also well-defined and interpreted in the same way by all parties.*

*Software vendors offering cloud solutions need to ensure and explicitly list the responsibility they take regarding these product specifications and service levels.*

”

# 09

---

## **Principle 9**

Commercial models shall not be changed unilaterally and shall adhere to an active 'opt-in' principle.

# COMMERCIAL MODELS SHALL NOT BE CHANGED UNILATERALLY AND SHALL ADHERE TO AN ACTIVE 'OPT-IN' PRINCIPLE.

## Description

### How vendors change their commercial models

Vendors often offer several software applications for distinct functions. Productivity software such as calculation, word processing, email and communication, operating systems, database management software, software for sharing and storing information, collaboration tools, virtualization software or security are all very different software applications. Yet, depending on the vendor, several of the applications may be owned by the same vendor. They repackage their commercially available software, change names and update functionality on a frequent basis. While customers do not object to improvements and updates to existing commercial offerings, challenges are created when a functionality or element is removed or customers are forced to incrementally invest in new products to follow the vendor's release cycles. The changes to the commercial models or functionalities should not have an adverse impact on the functionalities and commercial conditions initially selected and agreed upon. Vendors shall continue to offer at least the same functionality under the same contract terms and commercial conditions. Customers shall be able to rely on stable conditions for cost forecasting and application portfolio management purposes.

The practice of increasing the functionalities and increasing the prices under the same license name, combined with creating a new package with different functionalities, creates a need to constantly follow updates and, when necessary, to change to the new package, simply to keep the same functionalities. If this isn't done, the customer moves to the more comprehensive, more expensive package.

Maintenance and support shall be part of the software terms and commercial conditions. The period of the maintenance and support lifecycle and the rights included therein shall be transparently communicated upfront, and commercial conditions shall not be unilaterally changed.

Cloud providers apply various techniques that allow them to unilaterally modify the contract and conditions in cloud agreements to change prices or terms without negotiation, creating opacity and dependency for customers. This lack of transparency — often marked by unrealistic list prices or inconsistent tariffs — prevents clients from benchmarking or negotiating fair rates. As a result, customers face rising, non-negotiable costs and even the risk of contract termination if they resist, a situation that can constitute an abuse of dominance under Article 102(a) TFEU.

### Active opt-in, not opt-in-by-use

Commercially available features or changes that are subject to additional fees shall not be enabled by default. The customer shall be transparently notified before deployment and usage, or alternatively have the ability to actively opt-in. The customer shall be able to verify and prove non-usage of commercial features if they are activated but never intentionally used. The customer shall be able to apply corrective actions if such usage invoked a licensed feature without intent.

Customer employees or individuals working on behalf of the customer are typically technical resources who do not have the mandate to sign off on and commit to additional fees triggered by usage of the software.

### **Packages now include AI as a revenue driver**

Vendors are actively incorporating AI into their solutions, regardless of its effectiveness, as the market shifts to enhance visibility and prioritize technological advancements. However, technical implementation or value creation is frequently lacking, resulting in a lack of genuine value-add. Clients have no choice between packages with or without AI, vendors force clients into a situation of bundling and price increases. These price hikes often restrict clients' ability to invest in technologies or solutions that genuinely provide value.

## **Examples**

- A major software vendor increases prices under the claim of greater or improved functionality. However, it does not take into account the customer's usage or alternative packages to rationalize the costs. While the package may contain more functionalities, these are not customer driven. Furthermore, the old package is no longer offered or the customer has to change to a package with a different name but with the same bundled functionalities and at the same price. Instead of an active opt-in, the vendor applies an active opt-out.
- Other vendors enable add-ons or options to a base functionality by default. The add-ons and options trigger additional license costs. Customers shall have the ability to review and granularly select the functionalities to deploy and use.
- A customer invests in licenses for their employees to use several applications that are offered in a package or suite. The package license allows all employees to use these applications, which they do. At a certain moment, the supplier decides to divide the applications in the package across two different packages, each needing a license to use the applications. The customer now must re-invest in new licenses in order to make the same applications available to their employees. There is no added benefit, but twice the cost for the customer.



“ Cloud solution providers like to innovate and develop their products ... and increase the price, even if it doesn't have much value for the customers.

All this innovation happens unilaterally, and bundling and cross grading (the process of bringing users of a competitive product in a new release in a commercially attractive way) in particular cause a lot of issues and market distortion.

In the recurring payment model inherent to cloud computing, the customer shall be able to rely on stable conditions for cost forecasting and application portfolio management purposes.

Customers shall have the ability to review and granularly select the functionalities to deploy and use.

The ninth principle guarantees stability around cloud services and pricing; commercial models shall not be changed unilaterally and shall adhere to an active 'opt-in' principle.

”

# 10

---

## **Principle 10**

Commercial models and offerings shall be consistent and reasonable, not combining different models for the benefit of the vendor's revenue.

# COMMERCIAL MODELS AND OFFERINGS SHALL BE CONSISTENT AND REASONABLE, NOT COMBINING DIFFERENT MODELS FOR THE BENEFIT OF THE VENDOR'S REVENUE.

## Description

### Subscription model or perpetual license model, not both

Commercially available products under a subscription model (i.e. cloud-based) shall deliver the commercial flexibility and scalability being marketed. Subscriptions shall therefore be a flat fee: non-committed, flexible and pay-as-you-go. Vendors shall not require upfront investment or production usage fees during development and deployment.

Customers shall have the flexibility to reduce the number of licenses after each commitment term expires. During the committed term customers shall have the ability to scale up at the entitled price and eligible tiered pricing if applicable.

Software offered as a perpetual right-to-use model (i.e. licenses including maintenance) is a frontloaded investment, and can be considered an intangible asset. This provides upfront benefits for both customer and vendor. The subsequent maintenance shall be at an agreed and predictable fee for the customer. Customers shall not be forced to convert from a perpetual license model with maintenance to a subscription model during the same commitment term and without material changes to the solution's functionality. When software is purchased under a perpetual license model including maintenance, and provided the customer uninterruptedly continues the maintenance stream, the customer shall remain entitled to use the software, including all benefits of the maintenance (e.g. upgrades). Vendors shall not be allowed to change the commercial model when the customer has followed all the maintenance conditions.

Mixing models is detrimental for the customer value: converting from a perpetual to a subscription model benefits the vendor. The customer has made the initial investment in the perpetual license, after which the vendor switches to higher subscription charges. In addition, vendors requiring upfront investment under a subscription model attempt to frontload the investment, while the subscription does not represent a perpetual right to use (or intangible asset).

Applying multiple license models within the same organization creates inconsistencies and complexity in pricing, naming, and application management.

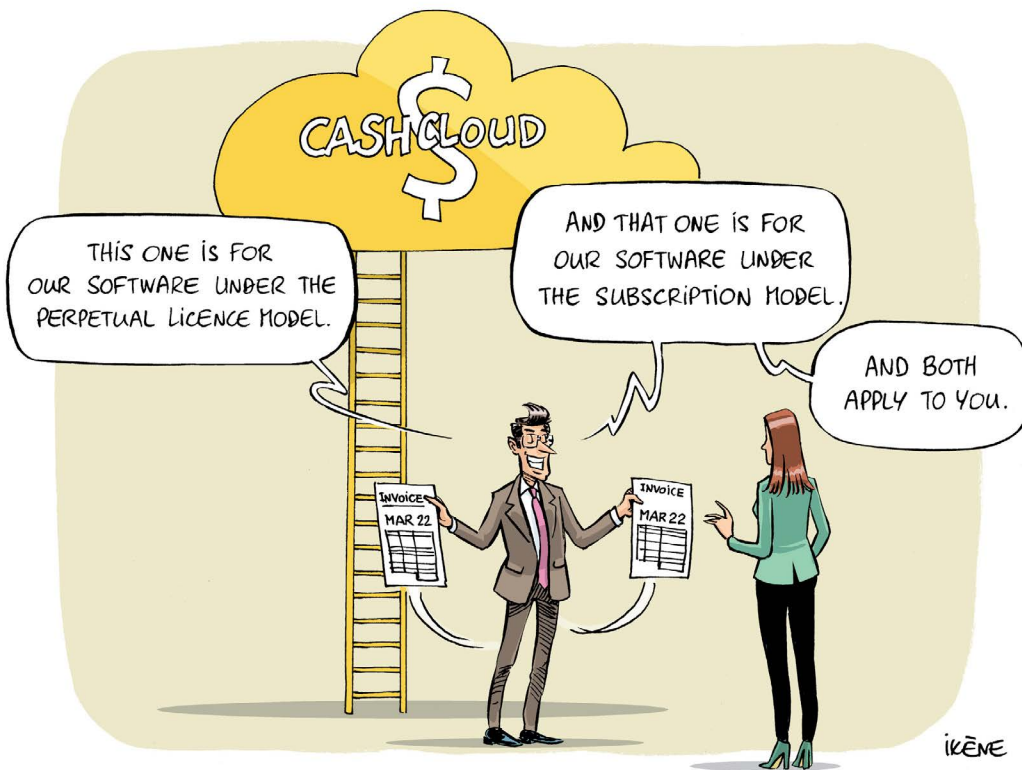
The customer has limited alternatives if the product is only continued under a subscription model: either run the software without maintenance and support or follow the vendor's conversion to subscription model.

### Licensing changing the basis for the calculation within the terms

In addition to conversions from license with maintenance to subscription model, some vendors also convert license per device to license per user for the same software, running on the same machines. It is clear that the use case needs to be completely re-analyzed if such a change is imposed.

## Examples

- A vendor obliged all existing customers with perpetual licenses to move to a subscription model. Before a specific date, the conversion was without cost. Afterwards, there was a 30% price increase. The vendor framed this forced move as an 'application modernization program'. Customers nevertheless wanted to remain with the previous version.
- The roll-out of digital meters has been negatively impacted by a change in metrics. An ERP vendor announced that, in addition to internal users, users connecting through the internet would be defined as users needing a license. When rolling-out the digital meters that eliminate the need to physically check millions of meters, utility companies were suddenly faced with a huge increase in users, obliging it to acquire millions of licenses. This change to include 'indirect' use led to enormous protest, but in the end business users had to increase the number of licenses and therefore costs.
- A drawing software vendor increased its client base by offering the best deal. Three years later, the vendor changed from perpetual licenses to a subscription model, giving its clients six months to move to the new model at a reduced price. Many companies changed to the new model. 12 months later, the vendor again changed the model, towards a license per user. One particular organization had 30 licenses, despite at no moment having more than 30 employees using the software at the same time. But, in total, 300 employees used the software, mostly to consult drawings rather than create them. Although the software vendor proposed converting the licenses 1-to-2 ratio towards named licenses, the organization now only gets 60 names, whereas before 30 licenses were enough. The organization would need five times more licenses under the new commercial model.
- A vendor supplies a connector between two major software packages. It offered a perpetual license combined with a maintenance contract. Without any move to the cloud or other underlying technological or architectural change, the vendor changed its commercial model to subscription-only, charging a subscription fee that exceeds the original maintenance costs. Consequently, the customer using the software simply has to pay more.
- A vendor changed its licensing model from device-based to machine-based. Depending on the use case, this change can have significant consequences for a company's business. If several people share a stock of machines, they can cope with peak periods by increasing the number of users without having to worry about the licensing. But when a license per user is required, having more people working with the same machines increases costs. As such, the licensing model determines the customer's business case.
- Following a recent acquisition, a leading infrastructure software vendor abruptly changed its licensing model, no longer valuing the client's initial investment in a perpetual license with maintenance. Instead, it consolidated the commercially offered packages (i.e. customers received additional functionalities they did not want), voided the perpetual licenses by stopping support unless clients converted to subscription models without compensation, and imposed a minimum subscription quantity that was oversized for most mid-size companies. The combination of contractual practices led to a price hike for clients up to 500% year over year. Some clients have taken legal steps against the contract changes, but few have done so due to fear for the continuity of their operation should the provider withdraw support as a punitive measure.



“

*Subscription model or perpetual license model, not both.*

*Customers shall not be forced to convert from a perpetual license model with maintenance to a subscription model during the same commitment term. Mixing models is detrimental for customer value. The customer has made the initial investment in the perpetual licenses, after which the vendor switches to recurring subscription charges.*

*The way in which software is licensed evolved. There are licenses per CPU, user, device, revenue, documents processed in a software, extra security features, etc. It became complex to calculate the licenses needed within an organization. On top of that, vendors change their models, requiring the use case to be completely re-analyzed.*

”

# 11

## **Principle 11**

The scope, execution and intended outcome of an audit shall be clearly defined in the contract.

# THE SCOPE, EXECUTION AND INTENDED OUTCOME OF AN AUDIT SHALL BE CLEARLY DEFINED IN THE CONTRACT.

## Description

Providers make such complex licensing models that the customer does not know how to comply. Then they audit the customer to find the flaws and impose penalties.

The right to audit in itself is not unfair if the customers formally agree to it in a contract. However, the outcome, timing, objectivity and intended purpose often go beyond the nature of a factual verification. In some cases, audits appear to have an additional aim of selling more licenses, promoting new products and services, or pressuring the customer to move to a new platform or business model. Audits shall not be misused for such ends.

When possible, software shall be self-regulating, ensuring it does not lend itself to misuse or overuse, reducing the effort required from the customer to prove compliance during an audit. The move to cloud has facilitated audits in some cases. During an audit, customers shall not be held liable for software that was installed by default but never used nor activated; for example, by a license key.

## Examples

In some cases, vendors use audits to pressure customers to pay for the increased usage they were not aware of or that arose due to the definition of the word 'use' (see principle 4). In other instances, audits occur close to or during contract negotiations, fueling the perception that they are being used to pressure the customer.

- A large software supplier wanted to conduct an audit but could not provide a correct list of current licenses. Licenses were attached to non-existent legal entities, legal predecessors that were no longer operational, or were not allocated correctly to entities after carve-outs.
- A supplier established some incompliance during an audit, and subsequently filed a substantial claim. The claim would only be reduced if new licenses were purchased for the product that had become the primary focus within the sales organization, regardless of whether the customer needed it.
- A supplier refused to accept the cost calculation method agreed upon by the intermediary/implementation partner with the customer, even after that calculation had been accepted by the supplier in writing at an earlier stage. This led to a non-compliance claim being filed, based on a near doubling of the application's use compared to the contract. The claim, however, was not twice the original cost but 20 times.

Here are three examples of increased use through the automatic provision of licenses when certain functions are used:

- A collaboration software automatically issues licenses to users whenever they are able to install it using a company email address. It is clear that the employees who organize meetings need a license, while those only join meetings don't. When a customer has a Bring Your Own Device (BYOD) policy for external consultants, who thereby temporarily receive a company email, this becomes a crucial issue. The external consultants don't organize meetings, they only participate. However, through a back door in the licensing policy, they will still get a license if they use the company email. During auditing or cloud use verification, the customer is notified that they have many more licenses than they provisioned for.
- A document sharing software vendor requires a license to send, but not to receive, documents. However, if a person receiving a document comments on it, the vendor requests a license, which is automatically provided. Again, during auditing or cloud use verification, customers are notified that they have many more licenses than they provisioned for.
- Audit clauses, while ostensibly designed to verify compliance with licensed usage rights, often grant suppliers disproportionate power to initiate audits unilaterally. In practice, this imbalance can lead to strategic misuse: providers may structure contracts or technical environments in a way that makes compliance verification complex; employ auditors lacking independence; or withhold formal certification to maintain pressure. By turning the audit process into a tool of coercion rather than verification, suppliers can exploit it to influence contract renegotiations and reinforce their dominant position.



“ *Business users are generally not against a contractually defined right to audit, but good agreements make good friends. Let us therefore conclude with this 11th and last principle: the scope, execution and intended outcome of an audit shall be clearly defined in the contract.* ”

”

## About us – Who we are

We are the Belgian, Dutch, French and German CIO associations; communities of Chief Information Officers (CIOs) and other senior leaders who are responsible for digital technologies and digital transformations within private or public organisations. These are all business users of digital technologies. We do not represent ICT suppliers and consultants.

 **Beltug**

Beltug - Belgium

**Cigref**  
SUCCEED  
WITH DIGITAL

Cigref - France

 **PLATFORM  
NEDERLAND**

CIO Platform - The Netherlands

**VOICE**  
Bundesverband der  
IT-Anwender e.V.

VOICE - Germany