EMBER ÉS JOG • 2025/1-2. • 79–101.

Ember és Jog Jogtudományi Folyóirat
www.proveritate.hu

Legal Frameworks and Market Dynamics of Cloud Computing Contracts: Analyzing Obligations, Liabilities, and Regulatory Challenges

Khraisha, Wasim[1]

[1] *Wasim Khraisha*. PHD student
[1] Karoli Gaspar University of The Reformed Church, Budapest, Hungary

Abstract: *This article explores the evolving legal and contractual landscape of cloud computing, focusing on the complexities of cloud service agreements and the legal responsibilities of various stakeholders. It provides a comprehensive analysis of cloud contracts, including Service Level Agreements (SLAs) and Data Processing Agreements (DPAs), and their role in allocating liability, managing risks, and ensuring compliance with key regulations such as the General Data Protection Regulation (GDPR) and the NIS2 Directive. The paper examines the implications of different deployment (public, private, hybrid, community) and service models (SaaS, PaaS, IaaS) on the content and enforceability of cloud contracts. It also considers emerging challenges posed by AI-generated and smart contracts and addresses dispute resolution, enforcement, and regulatory intervention, particularly within the European Union. Ultimately, it highlights the need for adaptable legal frameworks and robust contractual practices to ensure legal certainty, fairness, and data protection in a rapidly changing technological environment.*

KEYWORDS

Cloud Computing Contracts, Data Protection (GDPR), Service Level Agreements (SLAs), Liability and Risk Management, NIS2 Directive, Smart Contracts, and AI in Cloud Services

CITATION

KHRAISHA, Wasim: Legal Frameworks and Market Dynamics of Cloud Computing Contracts: Analyzing Obligations, Liabilities, and Regulatory Challenges. *Ember és Jog*, 2025/1-2. 79–101.

1. Introduction

In the last decade, cloud technology has dominated the digital market with its exceptional facilities that allow businesses and individuals alike to access their data through computing resources on demand in a timely manner. Multiple players are usually involved in cloud transactions, from the cloud services providers (CSPs), and the cloud customers to the end users. This makes it challenging to arrange and organize the obligations and liabilities arising during cloud operations and market transactions. Consequently, contractual agreements are the most important tool for determining and ruling the complex overlapping roles and responsibilities of the cloud players acting in the market. Cloud agreements such as cloud service agreements (CSAs) and service level agreements (SLAs) are primary mechanisms for governing these interactions. However, the varied nature of cloud services and the international scope of its providers and resources makes the regulatory structure surrounding cloud contracts Vague and complex. This article examines the legal nature and structure of cloud contracts while analyzing cloud market transactions and related liabilities. It will provide a comprehensive analysis of the legal frameworks governing cloud services contracts and explore their implications on market dynamics, liability structures, and regulatory compliance. Additionally, it will clarify the main provisions of responsibilities specified in the most related regulations of all parties involved in the cloud transactions. In addition, it will address emerging trends, such as the rise of AI-generated contracts and smart contracts, shedding light on the doctrinal and practical challenges they pose. Notably, since cloud computing is widely spread as a general-purpose technology, various questions are continuously emerging concerning contractual liabilities, legal compliance, and market competition. In our analysis, we will touch upon several of these related issues and more.

2. Understanding Cloud Contracts and Market Transactions

2.1. Legal and Contractual Challenges in Cloud Computing

Cloud computing could be defined as "Internet-based computing where various resources and services are available through a wide network access".[1] Although cloud technology offers multiple attractive features to customers, such as saving on expenses, quick deployment, flexible pricing, and high scalability, the technical and commercial arrangements for delivering cloud services are often complex and vague.[2] Cloud contract-related issues are a main concern for enterprises relying on cloud services, especially medium and small enterprises. A study conducted by the European Commission in 2018 shows that a quarter of the institutions involved in the study suffered from different cloud-related

[1] JAISWAL, Manishaben: Cloud Computing and Infrastructure. *International Journal of Research and Analytical Reviews*, 2017/2. 742–746.

[2] MICHELS, Johan David – MILLARD, Christopher – TURTON, Felicity: *Standard Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021. 73.

problems, most reported of them the low speed of the service, vague contract terms and provisions, one-sided changes in the contract or the service, data retrieve difficulties, and clauses that limit the provider's liability.[3] Thus, fixed and well-structured contractual agreements will be needed to properly handle and govern these issues, especially for big cloud customers. Cloud service contracts are an essential method for determining and allocating mutual responsibilities, liabilities, and other crucial clauses ruling the relationship of the parties involved.

2.2. Structure and Key Elements of Cloud Contracts

Typical cloud service agreements are usually presented by the standard terms of service (ToS) under which providers offer cloud computing services. However, these standard terms might not be sufficient in certain cases, especially when large customers are involved, raising the need for modifying them according to each situation.[4] Terms of service, in general, are "a documentation of the detailed overall relationship between the customer and the provider, stipulating commercial terms and governing legal aspects such as choice of law and disclaims".[5] It is to be noted that it usually consists of several integrated documents, which together formulate the ToS for the cloud computing service provided, such as a privacy policy document for the specification of the related provisions for the CSPs as processors and compliance with the concerning data protection regulation like the GDPR.[6] Plus an acceptable use policy document that restricts the customer's use of the service.[7] SALs or service level agreements are other crucial examples for cloud service contracting; they could be defined as "It is an agreement that clarifies the level of service the supplier should provide to the customer, placing measures that enable the evaluation of the service, compensations of incidents, and penalties when service levels agreed on not provided accordingly".[8] In cloud computing, it is an agreement governing the relationship between the CSPs and the Customers. It mainly consists of the service terms, which help the cloud customers to be aware and clarify the different aspects of the cloud ecosystem, its pros & cons, the multiple cloud-based services, the various deployment models, general security concerns, legal

[3] *Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts. Final report.* Brussels, European Commission, 2018.

[4] RADU, Bogdan: Key Aspects of Cloud-Computing Services Related Contracts. *National Strategies Observer,* 2016/1.

[5] MICHELS, Johan David – MILLARD, Christopher – TURTON, Felicity: Contracts for Clouds: An Analysis of the Standard Contracts for 40 Cloud Computing Services. *Queen Mary Law Research Paper Series*, No. 334/2020. 4.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[7] Ibid.

[8] OVERBY, Stephanie – GREINER, Lynn– PAUL, Lauren Gibbons: What Is an SLA? Best Practices for Service-Level Agreements. *CIO*, June 21. 2024.

liabilities and responsibilities, and guarantees of delivering the service.[9] Of utmost importance is the DPA or (Data Processing Agreement). It is a binding contract between the data controller, usually the cloud customer, and the data processor or the CSP. Its main function is to highlight the terms and conditions for processing personal data in compliance with related laws. DAPs are vital to guarantee that personal data is processed lawfully, fairly, and securely. It also helps to control and oversee the data that remains with the controller. Moreover, the demonstration that the data processor applies strict security and legal obligations, and lastly specifies obvious foundations for liability, data breaches, and third-party sub-processor. It is to be noted that the GDPR under Article 28 makes it compulsory for controllers and processors to conclude a DPA. Consequently, any data processing activities done without DPA in place will be considered illegal according to the GDPR and lead to significant fines of up to 20 million Euros or 4% of the annual turnover.[10]

Generally, in cloud service agreements, some popular terms constitute its overall build, most importantly the minimum standards availability, speed of performance, and communication that could be also described as the "performance of the cloud service provided". Stipulations concerning the right to change the service by the providers and remedies clauses are also typically included in cloud agreements for any service failures as they contribute to mitigating liability and reducing costs for the CSPs. Plus, Deadlines for acknowledgments, by which the CSP has to admit the customers' requests to handle related issues or problems. Warranty terms: usually, during the contract negotiations, the customers could ask the providers to include warranties on the performance of the service as agreed on. Additionally, Maintenance services by the CSPs, for instance, repair the technology. Also, Acceptance, rejection, and delivery terms enable customers to figure out if the service is functioning properly. In addition to audit rights, cloud customers may need to guarantee the right to evaluate the CSP's security system. Limitation of liability and exclusion of consequential damages clauses. As well as training clauses on how cloud customers should use the technology. Disaster recovery terms set out recovery procedures for disasters such as wars or natural disasters. Insurance clauses, it is very important to impose insurance obligations on the CSPs. Termination clauses are a crucial part of the cloud contracts for ensuring the customer's termination rights.[11] With regard to the DPAs, a GDPR-compliant DPA must include the scope and purpose of the data processed, the obligation of the processor, data security measures, sub-processing rules, data subject rights, data breach

[9] DASH, S. B. et al.: Service Level Agreement Assurance in Cloud Computing: A Trust Issue. *International Journal of Computer Science and Information Technologies,* 2014/3.

[10] GRYFFROY, Pieter: Legal Aspects of Multi-Cloud: More Clouds, More Problems? *C.T.L.R.*, 2018/5. 129–131.

[11] REYNAUD, Laura: Read Before Signing: 15 Terms in Cloud Service Agreements. *ACC Docket*, September 29. 2021.

notification, data transfer provisions, retention and deletion, audits and compliance, and liabilities with penalties clauses.[12]

2.3. Parties Involved and Their Responsibilities

Several parties shape cloud contracts and agreements. Special legal responsibilities and liabilities are classified for each of them. Drafting contractual agreements carefully contributes to making sure data protection regulations are respected and reducing risks in cloud layers. It will also contribute to all parties performing their responsibilities that are being understood by a contract.[13] The first party in the cloud services agreements is the Cloud Service provider (CSPs) or the corporation that offers cloud services like applications and storage, such as Google Cloud and Microsoft Azure.[14] Their legal responsibilities mainly revolve around adhering to data protection regulations and compliance with related regulations such as the GDPR, NIS2, and others. As well as ensuring the service level guarantees, encryption is an example. The other key party to cloud contracts is the cloud customer, which may include individual users or organizations. Individual customers typically use cloud services for personal purposes, for instance, consumers using Google Drive to store files or access cloud-based applications. Organizational customers, on the other hand, include private companies and public sector bodies that rely on cloud infrastructure to support their operations. Notably, many European Union institutions utilize Microsoft Cloud services, which necessitates strict compliance with EU data protection laws and the implementation of robust access control and security policies. Although data subjects or end-users) are not contracting parties of the cloud agreements, they have significant rights guaranteed by the GDPR provisions, subsequently, they could file complaints for any breaches occurring to their data by the cloud providers or customers. Third-party providers or cloud sub-processors are also commonly engaged in cloud transactions to provide particular sides of the cloud service like data centers or AI analytics services, Crucially, they must follow data protection rules imposed by the CSPs and the cloud customers. Article 28 of the GDPR stipulates that CSPs are obliged to reveal all sub-processors and ensure data processing agreements are in place. It is possible to negotiate and manage cloud services between CSPs and customers through cloud brokers (Intermediaries). They help to improve cloud usage, enhance security, and ensure compliance with contracts.[15]

[12] KUNER, Christopher et. al.: The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. *Maastricht Faculty of Law Working Paper*, 2021.

[13] *Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019)*. United Nations Commission on International Trade Law. https://uncitral.un.org/en/cloud/liability.

[14] *What Is a Cloud Service Provider?* https://cloud.google.com/learn/what-is-a-cloud-service-provider.

[15] HON, W. Kuan et. al.: *Negotiated Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021. 129–139.

2.4. Deployment and Service Models: Legal Implications

Cloud service agreements differ in their content based on the cloud deployment model used.[16] Generally, there are four cloud deployment models: Private, public, hybrid, and community clouds. The private cloud refers to the model where a single large or specific number of cloud customers are the owners or the operators of the cloud-relevant infrastructure. While they are shared between several customers in the public cloud. A mix of both the private and public models refers to the hybrid cloud. A good example to understand it is when an organization relies on a private cloud but, due to being overloaded, has to switch to the public cloud for the extra flow to guarantee a continuous service. Lastly, the community cloud is the same as the private cloud, but it is specified to a group of customers sharing similar interests, such as government agencies or financial institutions.[17] Each of these models has its implications for the contractual agreements of cloud services. In the public cloud, it is important to highlight that the providers are usually dominant large multinational corporations, for example: Microsoft Azure and Google Cloud, typically offer their services in what is called the "take it or leave it" model or in other words their service offers are based on non-negotiable ToS or SLA. As a result, cloud customers may face limitations and restrictions to negotiate and modify these standardized contracts. Moreover, customers, in this case, will have to trust and count on the provider's security measures and compliance certifications. Thus, it is necessary to evaluate the alignment of them following the applicable legal requirements such as the GDPR and the Cybersecurity Act, etc.[18] Unlike the private cloud, where the agreements are customized, they are usually adjusted according to the special needs of an organization, opening the door for more dominance from the customers over vital aspects like security controls and compliance obligations. Therefore, these contracts provide significant control over infrastructure and data for the contracting customer. The situation is a little more complex concerning the hybrid cloud, where multi-cloud models are involved and various parties are also engaged. Hence, contracts in issue will need to go through comprehensive negotiations to ensure contracts are addressing matters such as interoperability, data portability, and integration between multiple cloud environments, as a consequence, obvious allocations of each party's responsibilities and precise provisions for the best compliance of regulations of different jurisdictions and cloud environments.[19]

[16] SCRUGGS, Ron – TRAPPLER, Thomas – PHILPOTT, Don: *A 6-Step "How-To" Guide to Contracting for Cloud Services Includes a 137-Element Contracting Checklist*. Longboat Key, Government Training Inc., 2011. 23.

[17] MELL, Peter – GRANCE, Timothy: *The NIST Definition of Cloud Computing*. Gaithersburg, National Institute of Standards and Technology, 2011. 3.

[18] REED, Chris – CUNNINGHAM, Alan: *Ownership of Information in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 145–149.

[19] JANSEN, Wayne – GRANCE, Timothy: *Guidelines on Security and Privacy in Public Cloud Computing*. 6–7, 26–27.

Regardless of the deployment model utilized, cloud services come in three models: the SAAS, PAAS, and IAAS. Each model refers to distinct services provided, which are reflected in the relevant contract structures.[20] The SAAS refers to the delivery of software as a service via the internet, which is managed totally by the CSPs who give their customers permission to access and use these applications through a website. This model is the most simple to use by businesses, as they will not need any software maintenance and related updates. A common example of this is email platforms. PAAS refers to the supply of a platform that enables specialists to structure, run, and deploy applications without the need to manage the underlying infrastructure. In the IAAS, the CSPs supply the computing resources over the internet, such as servers, storage, and networking. The customers are given the entire command of the infrastructure, letting them handle operating systems, applications, and the data. It provides flexibility and control and, at the same time, simplifies the administration of physical hardware.[21] Cloud service models can influence contractual terms, obligations, and potential risks, aiding organizations in making informed decisions when negotiating cloud contracts, as each model used has different implications based on the services provided. For instance, the SAAS Contracts typically cover subscription fees, service availability, updates, and user access rights. Contracts focus on resource consumption, access, intellectual property, and third-party integrations in the PAAS model. In the IAAS, Contracts usually emphasize scalability, uptime guarantees, security compliance, and data sovereignty.[22]

3. Legal Qualification of Cloud Contracts

It is important to understand the legal qualification of cloud contracts to have a clear path for their enforceability, regulatory alignment, and the allocation of rights and obligations among their parties. These contracts have distinguished features due to the special and multi-layer nature of the cloud transactions, which make them different from general services agreements.[23]

3.1. Contract Classification: Service, License, or Hybrid Agreements

In general, cloud contracts particularly those involving Software-as-a-Service (SaaS) are more accurately characterized as service agreements rather than software licenses, unlike conventional software licenses, which transfer a right to use a specific copy of software, cloud services involve on-demand access to software that remains under the control of the Cloud

[20] HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: UK G-Cloud v1 and the Impact on Cloud Contracts. *Queen Mary School of Law Legal and Studies Research Paper,* No. 115/2012. 4–5.

[21] ODUMOSU, Damilola O.: Cloud Service Agreement: Salient Contractual Clauses and Its Practical Implications. 2018. https://ssrn.com/abstract=3276612. 8–10.

[22] *Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019)*. United Nations Commission on International Trade Law. https://uncitral.un.org/en/content/main-pre-contractual-aspects.

[23] Ibid. 12–14.

Service Provider (CSP). Users do not receive a copy of the software, nor do they obtain ownership rights; instead, they receive a right to remotely use services managed by the provider.[24] This distinction is crucial in jurisdictions where the classification of a contract affects applicable legal rules concerning liability, consumer rights, and intellectual property rights. [25] But, other contracts of cloud services like (PaaS) Platform-as-a-Service or (IaaS)Infrastructure-as-a-Service usually include licensing or leasing terms. Consequently, we see that cloud contracts are best understood as "hybrid agreements", with their legal qualification dependent on the dominant purpose of the arrangement and the specific terms agreed upon by the parties.[26]

3.2. Comparisons with Traditional IT/Software Contracts

Traditional IT contracts, especially those involving software development, licensing, or hardware leasing, are generally based on clearly defined supplies and a relative determination of the specific subject matter. On the other hand, cloud contracts are by their nature dynamic, involving continuous service provision, service updates, and other distinguished factors. Moreover, the degree or the nature of control in cloud agreements differs significantly from that in traditional IT contracts. Traditional software licensing typically installs and manages software locally, while with regard to cloud services contracts, the CSP keeps control over infrastructure, platform, and even over the application multipole layers. [27] Crucially, this generates implications for the allocation of risk, liability, and compliance responsibilities in the cloud ecosystem.[28] Another important distinction refers to the termination and data migration. Traditional IT contracts usually allow users to continue using licensed software after termination –of course, if the contract's terms allow this- while in cloud services contracts, these rights end completely once the contract has been executed and expired. It is to be noted that this often leads to complex issues around data retrieval, portability, and continuity in the cloud.[29]

[24] KRATOCHWILL, György: What is the Difference between a Software License Agreement and a 'Software as a Service' (SaaS) Agreement? *les Nouvelles*, 2021/3.

[25] RUSTAD, Michael L. – KAVUSTURAN, Elif: A Commercial Law for Software Contracting. *Washington and Lee Law Review*, 2019/2. 843–848.

[26] *Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019)*. United Nations Commission on International Trade Law. https://uncitral.un.org/en/content/main-pre-contractual-aspects.

[27] BRADSHAW, Simon – MILLARD, Christopher – WALDEN, Ian: Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *Queen Mary School of Law Legal Studies Research Paper,* No. 63/2010. 7–8.

[28] *Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019)*. United Nations Commission on International Trade Law. https://uncitral.un.org/en/content/main-pre-contractual-aspects. 4–6.

[29] GEYER, Andrew – MCLELLAN, Melinda: Strategies for Evaluating Cloud Computing Agreements. *Bloomberg Law Reports – Technology Law*, 2011/13.

These differences necessitate a strong legal analysis, where regulators are increasingly encouraged to adapt existing contract doctrines to accommodate the evolving nature of cloud-based commercial characteristics.

4. The Legal Personality of Cloud Actors

Cloud environments have multi-actors, where in addition to the CSP and the customer, other players may be involved, such as subcontractors, data centers, or services vendors. This complex structure raises questions regarding the legal personality of each of them.[30] According to normal practice in contract law, only parties to a contract can enforce its terms. However, in cloud agreements, third parties might be affected or may benefit from certain provisions (e.g., users within an enterprise, end-consumers, or subcontractors of the CSP). This gives attention to the question of whether cloud contracts can or should recognize third-party beneficiary rights, especially in relation to data subjects under the GDPR or end-users under consumer protection laws.[31] It is worth mentioning that in some cases, cloud arrangements may also involve what would be called "agency relationships", where intermediaries manage cloud services on behalf of a CSP. The legal implications of such relationships must be carefully delineated, as they affect liability, representation, and the enforceability of contractual obligations.[32] Additionally, the mixed contracts, such as those between CSPs and their subcontractors, often remain unshared with the cloud customer, raising transparency and accountability concerns. Despite the fact that regulations such as the NIS2 Directive and GDPR increasingly require clarity in these relationships, particularly concerning the processing of personal data and the determination of responsibility in case of breaches or incidents.[33]

5. Legal Frameworks for Cloud Services Contracts

The nature of Cloud computing services suggests the operation within a complex net of legal obligations that cover data protection, cybersecurity, and consumer rights in several EU digital regulations such as the GDPR, NIS2 directive, and others, as well as the general contract law. These legal frameworks together would contribute to shape the cloud computing agreements from the very beginning point of negotiations until the final resolutions of these contracts and would influence the allocation of responsibilities and liabilities among the cloud actors.[34]

---

[30] *Navigating Regulatory Challenges in Cloud Services Agreements*. 2024. https://www.sifma.org/wp-content/uploads/2024/03/SIFMA-BLG-White-Paper-Cloud-Services-Agreement-2024.pdf. 5.

[31] SCHWARTZ, Alan – SCOTT, Robert E.: Third-Party Beneficiaries and Contractual Networks. *Journal of Legal Analysis*, 2015/2. 331–334.

[32] KEMP, Richard: *Legal Aspects of Cloud Computing: Cloud Contracting. White Paper v1.0.* Kemp IT Law LLP, 2019. 5.

[33] SANDSTRÖM, Isabel: *The Impact of the NIS2 Directive on Subcontractors in the Transportation Sector*. Master's thesis. Luleå, Luleå University of Technology, 2024. 42–45.

[34] EUSTICE, John C.: Understanding Cloud Data Protection and Data Privacy. *Thomson Reuters*, 2024. https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing.

5.1. The GDPR and Cloud Contracts

The General Data Protection Regulation (GDPR) has had a deep impact on the structuring of cloud contracts, particularly in the context of data processing activities. Given that most CSPs act as processors on behalf of customer–controllers, cloud agreements must comply with Article 28 of the GDPR, which sets forth specific requirements for data processing agreements (DPAs). Several crucial rules are set to clarify the subject matter, duration, nature, and purpose of processing, as well as obligations concerning confidentiality, sub-processing, data subject rights, and data security.[35] It also mandates prompt breach notification procedures, where processors are obliged to notify controllers without undue delay upon becoming aware of a personal data breach.[36] Consequently, this would prompt the inclusion of detailed incident response and notification frameworks within cloud contracts. Moreover, the GDPR's extraterritorial scope suggests that CSPs offering services to EU data subjects, regardless of their location, must ensure that their contractual frameworks enable compliance with EU data protection rules. This includes clauses concerning international data transfers (e.g., SCCs or adequacy decisions) and audit rights for data controllers. As a result, it is highly advised to structure cloud service agreements according to the GDPR contractual clauses and rules as a standard practice.[37]

5.2. The NIS2 and the Cybersecurity Act: Cybersecurity responsibilities for CSPs

The NIS2 Directive,[38] which substitutes the original NIS Directive, imposes enhanced cybersecurity and risk management obligations on essential and important entities, including CSPs as digital service provides.[39] Under NIS2, cloud providers are required to implement technical and organizational measures to manage cybersecurity risks and prevent, detect, and respond to incidents.[40] These obligations, as a result, affect cloud contractual drafting by making it compulsory to include clauses that address incident reporting, service availability, and supply chain security. It also introduces the supervision and enforcement mechanisms that impose CSPs to demonstrate compliance, which, as a result, would influence the structure of cloud SLAs and audit provisions.[41] Similarly, the EU Cybersecurity Act (Regulation (EU) 2019/881) establishes a voluntary European cybersecurity certification

[35] HON, W. Kuan et. al. *op. cit.* 139–144, and REED, Chris: *Information Ownership in the Cloud*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021. 145–147.

[36] Article 33 of the General Data Protection Regulation ("GDPR").

[37] WUERMELING, Ulrich – OLDANI, Isabella: *Regulation of International Data Transfers in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021. 340–381.

[38] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

[39] VANDEZANDE, Niels: *Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor*. 2023. https://ssrn.com/abstract=4383118. 5.

[40] Article 21 of the NIS2.

[41] SCRUGGS – TRAPPLER – PHILPOTT *op. cit* 71.

framework, including schemes specifically designed for cloud services.[42] While these certifications are not mandatory to adopt, obtaining an EU cybersecurity certificate can enhance trust and market competitiveness, and certified providers may include this as a contractual guarantee of service quality and security levels.[43]

5.3. Consumer Protection and Transparency in B2C and B2B2C Models

In B2C (Business-to-Consumer)[44] and B2B2C (Business-to-Business-to-Consumer)[45] contexts, cloud services must follow consumer protection laws, which emphasize transparency, fairness, and redress mechanisms and measures. It is to be noted that in B2C, the CSPs directly bear responsibility for consumer protection laws, such as transparency, data rights under the GDPR, and contract fairness. In B2B2C, liabilities and data protection obligations may be shared or split between the CSPs and the customers, making contractual clarity and regulatory compliance even more crucial.[46]

In the EU, the "Consumer Rights Directive"[47] and "Unfair Contract Terms Directive"[48] provide important provisions in this regard, mainly where cloud services are offered to individual end-users. In these scenarios, cloud contracts must contain terms that are transparent, reasonable, and not unilaterally modifiable without proper measures and justifications. Therefore, terms such as those governing data usage, data access, service limitations, and contract termination must be clearly stipulated.[49] CSPs must also enable consumers to withdraw from contracts and ensure proper remedies in case of non-performance, data loss, or any other incidents that may occur in the cloud ecosystem for the data. Even in B2B2C, where a contract is with a CSP but the end-user is a consumer, there may be indirect regulatory effects. Cloud customers' operating platforms such as

[42] The EU Cybersecurity Act.

[43] VANDEZANDE *op. cit.* 12.

[44] B2C refers to transactions between a business and individual consumers. In the cloud computing context, this includes services like Google Drive, Dropbox, or iCloud, where the cloud provider offers storage, applications, or services directly to end-users. For Example: A consumer subscribes to Microsoft OneDrive for personal file storage.

[45] B2B2C refers to a layered business model where a cloud provider offers services to a business (the intermediary), which then provides those services to end-users or consumers. The cloud provider might not interact directly with the end-user, but its services are still part of the delivery chain. For Example: Amazon Web Services (AWS) provides infrastructure to a healthcare startup (business), which then offers a health-monitoring app to consumers.

[46] HOOFNAGLE, Chris Jay: *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*. Consumer Federation of America, 2010. https://consumerfed.org/pdfs/Cloud-report-2010.pdf.

[47] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[48] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[49] LOOS, Marco – LUZAK, Joasia: *Update the Unfair Contract Terms Directive for Digital Services European Parliament*. 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU%282021%29676006_EN.pdf? 22–26.

marketplaces or apps) must ensure their own compliance with consumer law, which may require Consecutive contractual provisions with the CSP to ensure the best performance and accountability.[50]

5.4. Contract Law Frameworks

In addition to the before-mentioned laws and regulations applicable to cloud contracts, fundamentally, cloud agreements are also governed by "General Contract Law", which provides the foundational and basic rules for contract formation, interpretation, and enforcement. The determination of the relevance of a particular legal regime needs to be followed or has to be applied depending on the law governing the contract, which is often specified in a choice-of-law clause –if there is such in the contract.[51]

At the international level, the Principles of European Contract Law (PECL) and the "UNIDROIT" Principles offer soft law guidance that can inform the interpretation of cloud agreements, especially in cross-border transactions and data flows. They help to emphasize general principles such as good faith, cooperation, and fair treatment principles that are increasingly relevant in the complex, evolving nature of the cloud ecosystems.[52] On the other hand, the national frameworks like civil codes and commercial laws, such as the German BGB and the French Code civil, establish detailed rules governing consent, liability, force majeure, and damages for cloud contracts. These frameworks may significantly affect the enforceability of particular contractual terms, such as exclusions of liability, limitations of remedies, or unilateral termination rights.[53]

6. Liability and Risk Management in Cloud Transactions

Despite the fact that cloud computing has become a crucial component of modern digital infrastructure, it also introduces complex types of legal and operational risks. As organizations increasingly rely on third-party CSPs for the storage, processing, and transfer of data, the legal implications of service disruptions, data breaches, and contract violations

[50] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data (Data Act).

[51] MICHELS, Johan David – MILLARD, Christopher: *Digital Assets in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021. 191–192.

[52] LANDO, Ole – BEALE, Hugh: *Principles of European Contract Law, Parts I and II*. The Hague, Kluwer Law International, 2000.

[53] BRADSHAW, Simon – MILLARD, Christopher – WALDEN, Ian: *Standard Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 43–64, and HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: *Negotiated Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 101–107, and HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: *Public Sector Cloud Contracts*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 108–141, and REED – CUNNINGHAM *op. cit.* 142.

become central concerns. Effective liability and risk management strategies are, therefore, critical to ensuring trust, compliance, and resilience in cloud-based transactions.[54]

6.1. Legal Risks in Cloud Transactions

Cloud transactions are inherently exposed to a range of legal risks that stem from the nature of the services and the reliance on remote infrastructure. Such risks may include:

- Data Loss: Data may be accidentally deleted, corrupted, or rendered inaccessible due to system failures, cyberattacks, or provider negligence. It is a very important risk to be focused on as it raises liability questions regarding the responsibility for backup and recovery mechanisms.[55]
- Service Downtime: Unscheduled downtime or performance degradation can severely affect business continuity. Whether caused by technical failure, maintenance, or malicious interference, such disruptions can lead to financial and reputational harm for the cloud customer.[56]
- Breach of Service Level Agreements (SLAs): SLAs often define minimum performance standards and response times. Failure to meet these agreed-upon terms may constitute a contractual breach, exposing the CSP to consequent liability.[57]
- Force Majeure Events: Natural disasters, geopolitical issues, or global pandemics may interfere with the cloud services delivery. While force majeure clauses are typically used to exclude liability, their scope and enforceability depend on national contract law and judicial interpretation.[58]

6.2. Liability Models in Cloud Services

The allocation of liability in cloud transactions can follow various legal models, each with its own implications for accountability and risk allocation: Strict Liability is one type of liability under which liability arises regardless of fault or negligence. Although not common in cloud agreements, strict liability may apply in specific sectors involving high-risk data (e.g., healthcare or financial data) or under specific regulatory regimes. Another class of liability is what is called "Fault-Based Liability", where the liability is assigned based on discovering a fault, negligence, or breach of contractual responsibilities. This approach

[54] CHANG, Henry: *Data Protection Regulation and Cloud Computing*. In CHEUNG, Anne S Y – WEBER, Rolf H (eds.): Privacy and Legal Issues in Cloud Computing. Cheltenham – Northampton, Edward Elgar Publishing, 2015. 26–42.

[55] RITTINGHOUSE, John W. – RANSOME, James F.: *Cloud Computing: Implementation, Management, and Security*. Boca Raton, CRC Press, 2010. 158.

[56] KHANDELWAL, Manish – SAINI, Hukum: *Review on Security Challenges of Cloud Computing*. International Conference on Advancements in Computing & Management (ICACM-2019). https://ssrn.com/abstract=3463271.

[57] *Cloud Computing. Benefits, Risks and Recommendations for Information Security*. European Network and Information Security Agency, 2009. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[58] HON, W. Kuan – HÖRNLE, Julia – MILLARD, Christopher: *Which Law(s) Apply to Personal Data in Clouds?* In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 246.

requires proof that the CSP failed to exercise reasonable care or failed to meet contractual obligations. Alternatively, a type of liability that would best fit the cloud transactions and their complex nature is the Shared Responsibility model: many cloud contracts adopt a shared responsibility model, where both the CSPs and the customer bear distinct obligations. For instance, the CSP may be responsible for physical infrastructure security, while the customer is accountable for managing access controls and data within the cloud environment. This model, promoted by major CSPs like AWS, Azure, and Google Cloud, complicates liability assessments but allows for clearer and robust risk allocation.[59]

6.3. Contractual Risk Mitigation Tools

To manage and mitigate liabilities that may arise during cloud transactions, parties to a cloud contract frequently rely on a range of contractual instruments. These clauses would help to define responsibilities, limit risks, and provide remedies. Indemnity Clauses are a type of contract term that require one party (usually the CSP) to compensate the other affected party for damages arising in specific situations, such as data breaches or IP infringement. They shift the financial burden of certain risks but must be carefully drafted to avoid ambiguity. Liability Caps are another common sort of clause that might be included in cloud contracts. Cloud Contracts often include limitations on the amount a party may bear in the event of a breach. These caps may be expressed as a fixed sum or limited to direct damages.[60] While they protect CSPs from excessive claims, courts may refuse to enforce them if they are deemed unreasonable or contrary to public policy.[61] Most importantly to mention is the Exclusion Clauses: These clauses seek to exclude liability for certain types of incidents, such as indirect or consequential damages (e.g., loss of profits or reputation). While common in the cloud, their enforceability depends on national legal systems and must comply with doctrines of fairness and good faith.[62] Also, it is worth mentioning the Audit and Compliance Rights, where customers often negotiate the right to audit the CSP's security practices or require third-party certifications (e.g., ISO 27001, SOC 2). Such rights provide a mechanism to assess ongoing compliance and reduce information asymmetry between the parties.[63]

7. Dispute Resolution and Enforcement

The legal landscape for cloud services - dispute resolution and enforcement has been in rapid change, as cloud service arrangements increasingly involve multiple jurisdictions, diverse legal systems, and complex contractual frameworks. Dealing with such related

[59] HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. *Queen Mary School of Law Legal Studies Research Paper*, No. 117/2012. 94–101.

[60] ODUMOSU *op. cit.* 10–19.

[61] BRADSHAW – MILLARD – WALDEN *op. cit.* 1–46.

[62] *Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019)*. United Nations Commission on International Trade Law. https://uncitral.un.org/en/content/main-pre-contractual-aspects.

[63] OPPENHEIM, Charles: Cloud law and contract negotiation. *El profesional de la información*, 2012/5.

disputes presents significant challenges. This section explores primary enforcement. The growing relevance of alternative dispute resolution mechanisms and the role of emerging case law and national regulators in shaping effective enforcement in the cloud services.

7.1. Enforcement Challenges: Jurisdiction, Choice of Law, and Cross-Border Litigation

Cloud computing services, by their nature, surpass the national jurisdictions. Data storage, processing, and access may occur in multiple jurisdictions simultaneously, making it difficult to determine clear jurisdictional competence. Traditional principles of private international law, such as Lex loci solutions or Lex contracts, may not adequately address the territorial ambiguity of cloud transactions.[64] Cross-border data flow is a core element of cloud services, thus, jurisdictional issues often arise when determining the competent court in cross-border disputes. For example, a cloud customer in the EU may find it difficult to initiate proceedings against a non-EU (CSP) that hosts data in multiple third countries like the US. The Brussels I Regulation (Recast) provides guidance on jurisdiction within the EU, but its applicability is limited in global contexts. Moreover, "choice of law clauses" included in cloud service agreements often designate the CSP's home jurisdiction, potentially disadvantaging users, especially SMEs and cloud customers, who may not have sufficient power to negotiate alternative terms.[65]

Cross-border litigation further complicates enforcement due to potential conflicts of laws, difficulties in obtaining evidence located in third-country data centers, and disparities in procedural rules. Furthermore, enforcement of foreign judgments may be problematic in jurisdictions lacking mutual recognition agreements, creating a barrier to effective remedies.[66]

7.2. Alternative Dispute Resolution (ADR) Mechanisms in Cloud Disputes

Recently, new emerging mechanisms such as the Alternative Dispute Resolution (ADR) have gained traction in cloud-related disputes due to the limitations of traditional litigation measures. Thus, mechanisms like Arbitration, mediation, and online dispute resolution (ODR) can offer faster, more flexible, and cost-effective alternatives to court proceedings for data-related disputes and incidents in the cloud ecosystem.[67] Beginning with Arbitration as it can provide more confidentiality and enforceability in dispute resolutions. Under the New

[64] KUNER, Christopher: Data Protection Law and International Jurisdiction on the Internet (Part 1). International Journal of Law and Information Technology, 2010/2. 176–193.

[65] REED, Chris: *Cloud Governance: The Way Forward.* In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 380–390.

[66] SVANTESSON, Dan Jerker B.: A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. *AJIL Unbound*, Volume 109/2015. 324, 330.

[67] HON, W. Kuan – MILLARD, Christopher: *How Do Restrictions on International Data Transfers Work in Clouds?* In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013. 270.

York Convention and the technical expertise of arbitrators, it is considered desirable and particularly attractive in the cloud industry.[68] However, some concerns are still arising regarding the imbalance of power in arbitration clauses drafted unilaterally by CSPs and the risk of limiting access to justice for weaker parties like SMEs and customers.[69] In addition to Arbitration, Mediation provides an opportunity for collaborative resolution, especially where long-term business relationships are at stake. Meanwhile, Online Dispute Resolution platforms, particularly within the EU (e.g., the EU ODR platform for consumer disputes), are becoming more relevant as digital commerce expands.[70]

8. Regulatory Frameworks and Their Market Impact on the Cloud Industry

In the current legal and regulatory landscape of the EU, several substantial evolutions have been taken in response to the growing usage of cloud services. Among the most important of these are the General Data Protection Regulation (GDPR) and the NIS2 Directive, both of which have an impactful influence on how cloud service contracts are drafted and enforced.[71] By its provisions, the GDPR came with strict obligations concerning data protection, accountability, and cross-border data transfers, prompting CSPs to incorporate detailed privacy terms and data processing agreements into their contracts with their customers.[72] On the other hand, the NIS2 Directive enhances cybersecurity levels, especially for essential and important entities like cloud providers, and requires the CSPs to maintain strong technical and organizational security measures; subsequently, it significantly affects market entry, compliance costs, and liability allocation in cloud services agreements.[73]

It is crucial to acknowledge that the European Union Agency for Cybersecurity (ENISA), established by the EU Cybersecurity Act, has influenced the shaping of cloud security standards. ENISA's guidance, along with the EU Cybersecurity Act (CSA)[74] provisions, boost the development and implementation of cybersecurity certification schemes, such as the EU Cloud Services Scheme (EUCS). Such schemes would contribute to building trust in cloud services by establishing verifiable security benchmarks, potentially influencing procurement

[68] TERAMURA, Nobumichi – TRAKMAN, Leon: Confidentiality and Privacy of Arbitration in the Digital Era: Pies in the Sky? *Arbitration International*, 2024/3. 280.

[69] *The Impact of Mandatory Arbitration Clauses in Commercial Agreements*. 2025. https://www.possingerlaw.com/the-impact-of-mandatory-arbitration-clauses-in-commercial-agreements/.

[70] MARTIC, Dusko: Online Dispute Resolution for Cloud Computing Services. *CEUR Workshop Proceedings*, 2013. 1105. 13.

[71] BALBONI, Paolo – FONTANA, Francesca: Cloud Computing: A Guide to Evaluate and Negotiate Cloud Service Agreements in the Light of the Actual European Legal Framework. *ICT Law Review*, 2013/1. 12–17.

[72] WUERMELING – OLDANI *op. cit.* 340–381.

[73] *NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems*. Brussels, European Commission, 2025.

[74] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and Regulation (EU) No 526/2013 on information and communications technology cybersecurity certification and repealing (Cybersecurity Act).

decisions and competition in both the public and private sectors.[75] It is also essential to mention that the EU Digital Markets Act (DMA)[76] introduces "market competition concerns" into the cloud market, especially with regard to "large online platforms", which the DMA introduced as "gatekeepers". The DMA seeks to ensure fair competition and prevent Unfair commercial practices such as data self-preferencing, bundling, or exclusionary contracting. As a result, regulatory scrutiny is not only reshaping contractual practices and technical compliance but also redefining the competitive dynamics of the cloud services market in the EU.[77]

9. Regulatory Frameworks and Their Market Impact on the Cloud Industry

Technological innovations may have a significant impact on cloud contracts. One promising example is the integration of smart contracts into cloud SLAs, enabled by blockchain technology, which allows for automated, self-executing agreements based on pre-defined conditions. However, they raise complex doctrinal questions concerning enforceability, jurisdiction, and the interpretation of code-based terms under traditional contract law.[78] Similarly, the emergence of AI-generated contracts, where AI tools draft or negotiate SLA terms, could be a useful way to conclude cloud agreements. However, it would lead to ambiguity or errors in the basic contract principles such as consent, intention, and liability.[79]

It is to be noted that most jurisdictions do not have comprehensive legal frameworks to regulate smart contracts and AI-generated agreements in general; instead, they rely on general contract law principles. This, as a result, creates legal uncertainty for enforcement, especially for cross-border data transfers. For instance, while some states in the US and the EU have recognized the legal application of smart contracts, their enforceability often depends on whether they meet traditional legal criteria such as offer, acceptance, and consideration. Moreover, AI-generated contracts introduce concerns about the transparency and interpretation of the drafting process. Consequently, if neither party fully understands the reasoning behind certain automatically generated clauses, it becomes difficult to assign

[75] *EUCS – Cloud Services Scheme*. European Network and Information Security Agency, 2020. https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf. 4-7.

[76] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[77] *Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets*. Brussels, European Commission, 2023.

[78]) LEVI, Stuart D. – LIPTON, Alex B.: An Introduction to Smart Contracts and Their Potential and Inherent Limitations. *Harvard Law School Forum on Corporate Governance*, May 26. 2018.

[79]) MEENU: The Impact of Artificial Intelligence on Contract Law: Challenges and Opportunities. *Indian Journal of Law*, 2024/2. 26–28.

liability or evaluate compliance with legal standards of fairness, particularly in unequal negotiations.[80]

10. Conclusion

Cloud contracts represent a dynamic intersection between technological innovation and legal doctrine. As cloud services become essential to modern digital infrastructure, contractual frameworks must evolve to address not only the operational issues of data processing, storage, and access but also the complex regulatory obligations and risks involved. The legal structuring of cloud contracts consisting of CSAs, SLAs, and DPAs is central to ensuring that responsibilities are clearly defined and that compliance with regulations like the GDPR and NIS2 is guaranteed. Furthermore, the deployment and service models adopted by CSPs significantly influence the content and flexibility of these contracts, particularly in subcontracting and cross-border data flow contexts.

At the regulatory level, the increasing scrutiny brought about by the GDPR, NIS2 Directive, Cybersecurity Act, and DMA reflects a broader direction towards accountability, transparency, and fairness in digital markets. These frameworks are actively reshaping the way cloud contracts are drafted and enforced, impacting not only compliance costs and market entry but also the balance of power between CSPs and their customers. Moreover, emerging technologies such as blockchain and AI are beginning to challenge traditional contract doctrines, raising questions about enforceability, legal faith, and liability in automated and algorithm-driven contractual environments. While these technologies offer promising efficiencies, they also require new legal interpretations and safeguards to ensure fairness, transparency, and accountability.

In the end, effective legal governance of cloud contracts necessitates an adaptive and integrated approach, one that aligns contractual practices with evolving technological capabilities and regulatory requirements. Future developments in law and policy must not only respond to current gaps but also anticipate the doctrinal and market implications of technological transformation in the cloud ecosystem.

[80] LEVI – LIPTON *op. cit.*

Bibliography

BALBONI, Paolo – FONTANA, Francesca: Cloud Computing: A Guide to Evaluate and Negotiate Cloud Service Agreements in the Light of the Actual European Legal Framework. *ICT Law Review*, 2013/1.

BRADSHAW, Simon – MILLARD, Christopher – WALDEN, Ian: Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *Queen Mary School of Law Legal Studies Research Paper,* No. 63/2010.

BRADSHAW, Simon – MILLARD, Christopher – WALDEN, Ian: *Standard Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

CHANG, Henry: *Data Protection Regulation and Cloud Computing*. In CHEUNG, Anne S Y – WEBER, Rolf H (eds.): Privacy and Legal Issues in Cloud Computing. Cheltenham – Northampton, Edward Elgar Publishing, 2015.

DASH, S. B. et al.: Service Level Agreement Assurance in Cloud Computing: A Trust Issue. *International Journal of Computer Science and Information Technologies,* 2014/3.

EUSTICE, John C.: Understanding Cloud Data Protection and Data Privacy. *Thomson Reuters*, 2024. https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing

GEYER, Andrew – MCLELLAN, Melinda: Strategies for Evaluating Cloud Computing Agreements. *Bloomberg Law Reports – Technology Law*, 2011/13.

GRYFFROY, Pieter: Legal Aspects of Multi-Cloud: More Clouds, More Problems? *C.T.L.R.*, 2018/5.

HON, W. Kuan et. al.: *Negotiated Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021.

HON, W. Kuan – HÖRNLE, Julia – MILLARD, Christopher: *Which Law(s) Apply to Personal Data in Clouds?* In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

HON, W. Kuan – MILLARD, Christopher: *How Do Restrictions on International Data Transfers Work in Clouds?* In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. *Queen Mary School of Law Legal Studies Research Paper*, No. 117/2012.

HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: UK G-Cloud v1 and the Impact on Cloud Contracts. *Queen Mary School of Law Legal and Studies Research Paper,* No. 115/2012.

HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: *Negotiated Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

HON, W. Kuan – MILLARD, Christopher – WALDEN, Ian: *Public Sector Cloud Contracts*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

HOOFNAGLE, Chris Jay: *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*. Consumer Federation of America, 2010. https://consumerfed.org/pdfs/Cloud-report-2010.pdf

JAISWAL, Manishaben: Cloud Computing and Infrastructure. *International Journal of Research and Analytical Reviews*, 2017/2.

JANSEN, Wayne – GRANCE, Timothy: *Guidelines on Security and Privacy in Public Cloud Computing*.

KEMP, Richard: *Legal Aspects of Cloud Computing: Cloud Contracting. White Paper v1.0.* Kemp IT Law LLP, 2019.

KHANDELWAL, Manish – SAINI, Hukum: *Review on Security Challenges of Cloud Computing*. International Conference on Advancements in Computing & Management (ICACM-2019). https://ssrn.com/abstract=3463271

KRATOCHWILL, György: What is the Difference between a Software License Agreement and a 'Software as a Service' (SaaS) Agreement? *les Nouvelles*, 2021/3.

KUNER, Christopher: Data Protection Law and International Jurisdiction on the Internet (Part 1). International Journal of Law and Information Technology, 2010/2.

LANDO, Ole – BEALE, Hugh: *Principles of European Contract Law, Parts I and II*. The Hague, Kluwer Law International, 2000.

LEVI, Stuart D. – LIPTON, Alex B.: An Introduction to Smart Contracts and Their Potential and Inherent Limitations. *Harvard Law School Forum on Corporate Governance*, May 26. 2018.

LOOS, Marco – LUZAK, Joasia: *Update the Unfair Contract Terms Directive for Digital Services European Parliament*. 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU%282021%29676006_EN.pdf?

MARTIC, Dusko: Online Dispute Resolution for Cloud Computing Services. *CEUR Workshop Proceedings*, 2013. 1105.

MEENU: The Impact of Artificial Intelligence on Contract Law: Challenges and Opportunities. *Indian Journal of Law*, 2024/2.

MELL, Peter – GRANCE, Timothy: *The NIST Definition of Cloud Computing*. Gaithersburg, National Institute of Standards and Technology, 2011.

MICHELS, Johan David – MILLARD, Christopher: *Digital Assets in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021.

MICHELS, Johan David – MILLARD, Christopher – TURTON, Felicity: Contracts for Clouds: An Analysis of the Standard Contracts for 40 Cloud Computing Services. *Queen Mary Law Research Paper Series*, No. 334/2020.

MICHELS, Johan David – MILLARD, Christopher – TURTON, Felicity: *Standard Contracts for Cloud Services*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021.

ODUMOSU, Damilola O.: Cloud Service Agreement: Salient Contractual Clauses and Its Practical Implications. 2018. https://ssrn.com/abstract=3276612

OPPENHEIM, Charles: Cloud law and contract negotiation. *El profesional de la información*, 2012/5.

OVERBY, Stephanie – GREINER, Lynn– PAUL, Lauren Gibbons: What Is an SLA? Best Practices for Service-Level Agreements. *CIO*, June 21. 2024.

RADU, Bogdan: Key Aspects of Cloud-Computing Services Related Contracts. *National Strategies Observer,* 2016/1.

REED, Chris: *Cloud Governance: The Way Forward*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

REED, Chris: *Information Ownership in the Cloud*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021.

REED, Chris – CUNNINGHAM, Alan: *Ownership of Information in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 1st edition. New York, Oxford University Press, 2013.

REYNAUD, Laura: Read Before Signing: 15 Terms in Cloud Service Agreements. *ACC Docket*, September 29. 2021.

RITTINGHOUSE, John W. – RANSOME, James F.: *Cloud Computing: Implementation, Management, and Security*. Boca Raton, CRC Press, 2010.

RUSTAD, Michael L. – KAVUSTURAN, Elif: A Commercial Law for Software Contracting. *Washington and Lee Law Review*, 2019/2.

SANDSTRÖM, Isabel: *The Impact of the NIS2 Directive on Subcontractors in the Transportation Sector*. Master's thesis. Luleå, Luleå University of Technology, 2024.

SCHWARTZ, Alan – SCOTT, Robert E.: Third-Party Beneficiaries and Contractual Networks. *Journal of Legal Analysis*, 2015/2.

SCRUGGS, Ron – TRAPPLER, Thomas – PHILPOTT, Don: *A 6-Step "How-To" Guide to Contracting for Cloud Services Includes a 137-Element Contracting Checklist*. Longboat Key, Government Training Inc., 2011.

SVANTESSON, Dan Jerker B.: A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. *AJIL Unbound*, Volume 109/2015.

TERAMURA, Nobumichi – TRAKMAN, Leon: Confidentiality and Privacy of Arbitration in the Digital Era: Pies in the Sky? *Arbitration International*, 2024/3.

VANDEZANDE, Niels: *Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor*. 2023. https://ssrn.com/abstract=4383118.

WUERMELING, Ulrich – OLDANI, Isabella: *Regulation of International Data Transfers in Clouds*. In MILLARD, Christopher (ed.): Cloud Computing Law. 2nd edition. New York, Oxford University Press, 2021.

Other sources

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

Cloud Computing. Benefits, Risks and Recommendations for Information Security. European Network and Information Security Agency, 2009. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts. Final report. Brussels, European Commission, 2018.

The Impact of Mandatory Arbitration Clauses in Commercial Agreements. 2025. https://www.possingerlaw.com/the-impact-of-mandatory-arbitration-clauses-in-commercial-agreements/

Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, and repealing Directive (EU) 2016/1148 (NIS2 Directive)

EUCS – Cloud Services Scheme. European Network and Information Security Agency, 2020. https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf

Navigating Regulatory Challenges in Cloud Services Agreements. 2024. https://www.sifma.org/wp-content/uploads/2024/03/SIFMA-BLG-White-Paper-Cloud-Services-Agreement-2024.pdf.

NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems. Brussels, European Commission, 2025.

Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019). United Nations Commission on International Trade Law. https://uncitral.un.org/en/cloud/liability

Notes on the Main Issues of Cloud Computing Contracts (prepared by the UNCITRAL secretariat, 2019). United Nations Commission on International Trade Law. https://uncitral.un.org/en/content/main-pre-contractual-aspects

Regulation (EU) No 526/2013 on information and communications technology cybersecurity certification and repealing (Cybersecurity Act)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data (Data Act)

Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets. Brussels, European Commission, 2023.

What Is a Cloud Service Provider? https://cloud.google.com/learn/what-is-a-cloud-service-provider