STUDIA IURIS

Jogtudományi Tanulmányok / Journal of Legal Studies

2025. II. évfolyam 2. szám

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.
A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.
A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.
A folyóirat online verziója szabadon letölthető (open access).

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola
Székhely: 1042 Budapest, Viola utca 2-4
Felelős Kiadó: Tóth J. Zoltán

A tipográfia és a nyomdai előkészítés: Csernák Krisztina (L'Harmattan) munkája
Nyomdai kivitelezés: Prime Rate Zrt., felelős vezető: Tomcsányi Péter

Honlap: https://ajk.kre.hu/index.php/jdi-kezdolap.html
E-mail: doktori.ajk@kre.hu
ISSN 3057-9058 (Print)
ISSN 3057-9392 (Online)
URL: KRE ÁJK - Studia Iuris
https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html

REGULATING THE CLOUD IN THE EU: A COMPREHENSIVE REVIEW OF THE GDPR, NIS2, DSA, DMA, AND CYBERSECURITY FRAMEWORKS

FELHŐALAPÚ SZABÁLYOZÁS AZ EU-BAN: ÁTFOGÓ ÁTTEKINTÉS A GDPR, NIS2, DSA, DMA ÉS A KIBERBIZTONSÁGI KERETRENDSZEREK VONATKOZÁSÁBAN

Wasim Khraisha[1]

ABSZTRAKT ■ Az utóbbi évtizedben a felhőalapú számítástechnika szabályozása az EU hivatalos testületeinek egyik fontos kérdésévé vált. Több lépés és kezdeményezés történt ebben az irányban. Ez érthető, ha figyelembe vesszük a felhőalapú szolgáltatások hatalmas lehetőségeit, amelyek nemcsak a magánszemélyek, hanem a közérdek számára is fontosak. Jelen tanulmány átfogó áttekintést ad a felhőalapú tranzakciókra vonatkozóan alkalmazható jogszabályok egy részéről, különös figyelmet fordítva az adatvédelmi és biztonsági kérdésekre, a CSP-k kötelezettségeire, a piaci megállapodásokra és a felhőalapú infrastruktúra általános ellenálló képességére. Főként a GDPR, NIS2, DSA, DMA, valamint a Kiberbiztonsági Törvény kerülnek ismertetésre. A cél egy kritikai, de hasznos áttekintés nyújtása a jogszabályok összefüggéseiről és kölcsönhatásaikról a felhőalapú-ökoszisztémában. Ezenkívül a felmerülő kihívások és következmények is tárgyalásra kerülnek. A cél, hogy felfedjük az esetleges hiányosságokat vagy hézagokat, és végül olyan hatékony ajánlásokat tegyünk mind a felhőalapú szolgáltatók, mind az érdekelt felek számára, amelyek erős, ugyanakkor könnyen követhető megfelelőségi keretrendszert biztosítanak, elősegítve az innovációt és garantálva a felhasználók jogait a felhőalapú környezetekben.

Kulcsszavak: felhőalapú számítástechnika, adatvédelem, felhőalapú szabályozás, adatmegfelelőség, GDPR

ABSTRACT ■ During the last decade, the regulation of cloud computing has become a concern for the EU official bodies. Several steps and initiatives have been taken in this respect. This is understandable when looking at the huge facilities that cloud services provide, not only for private users but also for public interests. This paper comprehensively reviews some of

[1] PhD student, Doctoral School of Law and Political Sciences, Károli Gáspár University of the Reformed Church in Hungary.

the laws relatively applicable to cloud transactions in terms of data privacy & security, CSPs obligations, market arrangements, and overall resilience of the cloud infrastructure. Mainly, it will address the GDPR, NIS2, DSA&DMA, and the Cybersecurity Act. Aiming to give a critical but useful overview of their links and interplays in the cloud ecosystem. In addition, the challenges as well as the consequences that may arise from that. Leading to discovering any gaps or shortness to help at the end, offering some impactful recommendations for both cloud actors and stakeholders to ensure a strong but easy-to-follow compliance framework that improves innovation but guarantees users' rights in the cloud environments.

Keywords: cloud computing, data protection, cloud regulations, data compliance, GDPR

1. Introduction

Technological innovation without a doubt is, a major driver of economic growth and human progress. Several classification models are available to distinguish different types of technologies. A particular class of technologies is called general-purpose technology, which refers to those innovations whose impact and adoption span all sectors of the economy, improving and altering many pre-existing social and economic structures. The best examples of such technologies are electricity and information technology. In this regard, a technology called (cloud computing) has recently emerged as a powerful general-purpose technology with a substantial impact on all private and public sectors, promoting efficiency, competition, innovation, and growth. Briefly, cloud computing could be defined as *"the development and delivery of scalable, on-demand computing services, including computing machines, databases, storage, networking, software, analytics, and intelligence over the Internet"*.[2]

Cloud technology brings a large number of benefits. On the consumers' side, for example, they can synchronize and access their data across many devices, independently of the location, similar to how they already do with their emails and social media. For services like hospitals, the adoption of the cloud can facilitate the efficiency of services through data sharing. For example, people can have their medical history data stored in the cloud and made available to all hospitals. Education is another sector that benefits from cloud adoption, as lectures can be offered remotely (e-learning). The same applies

[2] Richard G. Lipsey – Kenneth I. Carlaw: *Economic transformations: general-purpose technologies and long-term economic growth*. Oxford University Press, 2005, https://www.researchgate.net/publication/227468040_Economic_Transformations_General_Purpose_Technologies_and_Long-Term_Economic_Growth (Accessed: 22/12/2024).

to public offices, defense, and any other sectors. On the other side, firms will be able to acquire as much computing and storage power as they need and pay only for what they consume, thus removing the need to maintain expensive infrastructure. Internally, the adoption of the cloud can increase productivity and collaboration (e.g., through instant data sharing), provide complementary support to improve creativity, reduce time-to-market, and create many other competitive advantages.[3]

Cloud computing regulations are still in their early versions. Many efforts are still required to create comprehensive frameworks and policies. For example, a study conducted by the European Commission to analyze the laws and contracts related to the cloud market in 28 European countries concluded that no specific cloud market laws exist in any of these countries.[4] In most cases, cloud-computing issues are dealt with in commercial contracts and rely on numerous laws drawn to related topics like data security and privacy laws, data transfer laws, and others.[5]

The lack of specific laws regulating the cloud, combined with the fast and wide adoption of this technology worldwide. There are two important reasons why cloud-computing regulation is a crucial domain to search in. This paper employs a qualitative research methodology to analyze key EU regulations affecting the cloud market. Specifically, the General Data Protection Regulation (Regulation [EU] 2016/679, hereinafter: the GDPR). Directive on measures for a high common level of cybersecurity across the Union (Directive [EU] 2022/2555, hereinafter: the NIS2 Directive). Digital Services Act (Regulation [EU] 2022/2065, hereinafter: the DSA). Digital Markets Act (Regulation [EU] 2022/1925, hereinafter: the DMA). Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Regulation [EU] 2019/881, hereinafter: the Cybersecurity Act). This article will give a comprehensive review of how these regulations interact and their possible implications for cloud service providers and customers.

[3] Joe Weinman: *Cloudonomics. The business value of cloud computing.* John Wiley & Sons, 2012.

[4] https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/study-economic-detriment-unfair-and-unbalanced-contractual-terms_en (Accessed: 28/12/2024).

[5] Vineeth Narayanan: Harnessing the cloud: international law implications of cloud computing. *Chicago Journal of International Law*, 2012 (2), 783.

2. Cloud Computing Models

Cloud computing has two types of models: the deployment model, which could be one of three types: public[6], private[7], or hybrid[8] cloud. And the service model, in three categories: IAAS, PAAS, and SAAS. IAAS: refers to infrastructure as a service. It is a cloud service model where users can get access to basic computing infrastructure. IT administrators commonly use them if the organization requires resources like storage or virtual machines. IAAS is the model that requires you only to manage the data, runtime, and middleware applications while the cloud providers handle the rest.[9] PAAS refers to the platform as a service. It provides cloud platforms and a runtime environment for developing, testing, and managing applications. This service model enables users to deploy applications without the need to acquire, manage, and maintain the related architecture. Whereas if the organization needs a platform for creating software applications, PAAS is the suitable model. PAAS only requires handling the applications and the data. The cloud service providers handle the rest of the components like runtime, middleware, operating systems, servers, storage, and other things.[10] SAAS refers to software as a service. It involves cloud services for hosting and managing software applications. The vendors satisfy software and hardware requirements, so no need to manage any of those aspects of the solution and no need for any IT equipment. With the SAAS model, the cloud service provider handles all components of the solution required by the organization.[11]

[6] In public cloud, the cloud infrastructure is available to the public over the internet, which are owned by cloud service providers, where resources are shared among multiple tenants, offering high scalability but less control, Giulio D'Agostino: *Data security in cloud computing volume*. Vol. I. New York, Momentum Press, 2019, 19.

[7] With private cloud, the cloud infrastructure is exclusively operated by a single organization, which could be managed by organization or a third party, usually private cloud is Dedicated to a single organization for enhanced security and compliance, Preston De Guise: *Data protection: Ensuring data availability*. London, CRC press, 2020, 217.

[8] The hybrid cloud is a combination of the functionalities of both public and private cloud, De Guise 2020, 220.

[9] Kevin McGillivray: *Government Cloud Procurement*. Cambridge University Press, 2022, 22.

[10] Theo Lynn – John G. Mooney et al.: *Data Privacy and Trust in Cloud Computing*. Palgrave Macmillan, 2021, 7.

[11] De Guise 2020, 211-212.

3. Adoption Trends in the EU

Not long ago, the adoption of cloud services grew gradually and significantly within the EU, due to the facilities that the cloud provides to all public and private institutions. A survey conducted on the adoption rates of cloud services in the EU says that at the end of 2023, about 45% of the corporations in the EU are relying on cloud services. In countries like Finland, Sweden, and Denmark, the rates were 78%, 72%, and 70%, respectively. While in Bulgaria and Romania, the average was 18% for both being at the bottom of the list.[12] Cloud technologies are also popular among public sectors as well, for example, in healthcare, education, and administrative services.[13] Leaning on the cloud contributes to saving expenses, ease of expansions, and developments for institutions. Moreover, they can anticipate approximately 20-30 % savings in their daily-related tasks, as well as enhancing marketing and helping achieve high economic performance.[14]

4. The General Data Protection Regulation (GDPR)

"Cloud services are naturally subject to the GDPR provisions, either on the side of the cloud provider, the customer, or both".[15] The GDPR came with several rules, concepts, and obligations, which together would constitute a safeguard for a secure environment for data in the cloud. Mainly on data privacy sides. Its primary purpose is to ensure the fundamental rights and freedoms of natural persons, particularly their right to data privacy, while ensuring the free movement of personal data within the EU. We see this closely connected with the CSPs, as it underscores the dual responsibility of protecting personal data and facilitating its lawful movement since cloud operations often involve cross-border data transfers and processing in multiple jurisdictions. Therefore, we see that CSPs must design their services in alignment with these principles, enabling secure and compliant data management while supporting data portability and mobility across the EU.

12 Market Trends of Europe Cloud Computing Industry, online report. https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market/market-trends (3/1/2025).

13 Europe Cloud Computing Market Size, online report. Source: https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market (3/1/2025).

14 Europe Cloud Computing Market Size, online report. Source: https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market (3/1/2025).

15 Christopher Millard: *Cloud Computing Law*. Oxford University Press, 2021, 384.

For example, encryption and data minimization are techniques that align with the GDPR's objectives.[16]

Key GDPR definitions are crucial for understanding its application to cloud computing. Data processing encompasses any operation performed on personal data, including collection, storage, retrieval, or erasure.[17] This broad definition covers a wide range of cloud activities, from basic data storage to complex analytics and machine learning. In most cases, enterprises using cloud services act as data controllers, responsible for ensuring compliance with GDPR requirements.[18] Processors, typically Cloud Service Providers (CSPs), process personal data on behalf of the controller, following the controller's instructions and ensuring data security and compliance.[19] A personal data breach refers to any security incident leading to the unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data, which is especially relevant in cloud environments due to the risks of hacking, data loss, or insider threats.[20] Such breaches must be managed following the breach notification requirements outlined in Articles 33 and 34 of the GDPR. Cross-border processing refers to the processing of personal data that takes place across multiple EU Member States or involves data transfers outside the EU.[21] This is particularly common in cloud operations and is critical for assessing compliance with the GDPR's rules on international data transfers, as outlined in Articles 44-50.

CSPs must take the burden of ensuring the processing they conduct is following the legal basis. Thus, they have to introduce their services following these principles, such as transparency, storage limitation, etc.[22] They must acknowledge a valid legal ground, such as contractual necessity, consent, or legitimate interests, for processing data legally.[23] In this subject, data processing agreements (DPAs), which are usually concluded between the CSPs and the customer, are vital for defining the conditions of processing and best compliance.[24] The GDPR recommended a written contract governing a relationship concerning data processing, detailing key aspects like the scope of processing, duration, data categories, and processing objectives & elements. This would be highly and directly relevant to cloud environments where data storage, processing, and

16 Article 1 point 1-3 of the GDPR.
17 Article 4 point 2 of the GDPR.
18 Articles 4 point 7 and point 24 of the GDPR.
19 Article 4 point 8 of the GDPR.
20 Article point 12 of the GDPR.
21 Article 4 point 23 of the GDPR.
22 Article 5 of the GDPR.
23 Article 6 of the GDPR.
24 Article 28 of the GDPR.

transfer are fundamentals.[25] Essential conditions for using sub-processors that are common in the cloud ecosystem require explicit general authorization from the controller and ensure equivalent data protection commitments across the service lifecycle.[26] In the end, they must securely return or erase data, aligning with service principles in cloud operations.[27] Data controllers and processors[28] must execute appropriate technical and organizational practices to maintain a level of security appropriate to possible risks, considering the nature, scope, context, and purposes of the processing.[29] These must include the *"ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services"*.[30] It also mandates the restoration of data availability and access in the event of a physical or technical incident. Additionally, regular testing, assessment, and evaluation of the effectiveness of security measures are necessary.[31] Crucially, on the matter of data breaches, controllers and processors must notify the competent data protection supervisory authority of a personal data breach within 72 hours of knowing it.[32] CSPs must notify the controller of any breach, who then informs the supervisory authority and data subjects, if necessary.[33] Given the shared and multi-layered infrastructure in the cloud, clear contractual agreements between the provider and client are essential to define breach notification responsibilities.[34]

Cross-border data transfer to third countries or international organizations might be the most critical challenge that may occur during cloud operations. Since data is stored across multiple cloud centers, which are usually located in different jurisdictions.[35] GDPR regulates this issue and provides many related essential resolutions. Any data transfer outside of the EU territories must comply with these obligations.[36] As a rule, data transfer to any third country or international organization is only allowed if a level of adequate protection is guaranteed, upon a decision on that from the European Commission based on specific elements.[37] Moreover, some useful tools are introduced to facilitate

25 Articles 28 point 2, point 3, subpoint (a), (b) of the GDPR.
26 Article 28 point 4 of the GDPR.
27 Article 2 point 3 subpoint (e), (g) of the GDPR.
28 Cloud customers and CSPS respectively.
29 Article 32 point 1 subpoint (a), (b) of the GDPR.
30 Article 32 point 1 subpoint (c) of the GDPR.
31 Article 32 point 1 subpoint (d) of the GDPR.
32 Article 33 point 1 of the GDPR.
33 Articles 33 point 2, Article 34 of the GDPR.
34 Article 33 point of the GDPR.
35 Millard 2021, Ibid.
36 Article 44 of the GDPR.
37 Article 45 of the GDPR.

transfers to the inadequate protection level countries, for example, the Standard Contractual Clauses (SCCs) or the Binding Corporate Rules (BCRs).[38] However, some exceptions are provided, like explicit consent from the data subject on his data transfer.[39] Notably, the commission and supervisory authorities should regularly assess the overall effectiveness of transfer mechanisms.[40] Such rules and provisions may be useful to limit foreign laws from overriding the GDPR.[41] Upon the previous explanation, we ensure that for secure cloud environments, clear contract terms are required to ensure compliance with cross-border data transfer rules.

The inherent risks associated with the vast amounts of data processed in the cloud, cross-border data transfers, and the potential for unauthorized access necessitate the implementation of a Data Protection Impact Assessment (DPIA). This process allows controllers or cloud customers to systematically identify, assess, and mitigate risks linked to cloud data processing activities. The GDPR requires consultation with supervisory authorities when risks cannot be mitigated, ensuring regulatory oversight of high-risk cloud operations. Article 35 of the GDPR thus establishes a proactive, risk-based compliance framework that aligns with the regulation's goal of safeguarding personal data.[42]

Two additional essential concepts for cloud compliance are Data Protection by Design and Data Protection by Default. These principles require data controllers to integrate data protection measures into the design of processing systems and operations from the outset. In cloud environments, this involves implementing technical and organizational measures to secure personal data and protect data subjects' rights. Additionally, it ensures that only the minimum necessary data is processed by following the principles of data minimization and purpose limitation. This approach fosters accountability and strengthens compliance with GDPR standards in cloud services.[43]

The GDPR is central to data security and privacy in the cloud, but its application presents several challenges. While it requires organizational and technical measures for data security, it lacks specific guidelines, leaving ambiguity for cloud transactions. The distinction between controller and processor roles becomes complex in hybrid or multi-tenant clouds, leading to uncertainty in liability. Additionally, the strict rules on cross-border data transfers complicate continuous

38 Article 47 of the GDPR.
39 Article 49 of the GDPR.
40 Article 50 of the GDPR.
41 Article 48 of the GDPR.
42 Millard 2021, 355-358.
43 Article 25 of the GDPR.

compliance throughout the data lifecycle. Finally, the GDPR's extraterritorial application creates challenges for cloud service providers handling data in non-EU jurisdictions, slowing compliance enforcement.

5. Network and Information Systems Directive, the NIS2

The NIS2 constitutes the second pillar of the EU's legal framework for data security in the cloud. It replaced the original NIS directive (Directive (EU) 2016/1148). It focuses on cybersecurity and the resilience of digital services to maintain appropriate measures in the face of cyber risks. In addition, it has wide applicability in numerous digital infrastructure sectors and is compatible with the growing need for suitable cybersecurity measures in cloud environments.

One of the most important goals of this directive is to harmonize cybersecurity requirements within the EU. Exceptionally, it provides a more consistent compliance framework for CSPs operating in multiple jurisdictions.[44] For multinational cloud providers, these unified standards reduce the costs and challenges of compliance while enhancing security levels for users.[45] The NIS2 directive gave the CSPs a special definition as "Essential Entities",[46] determining their important contributions to the digital markets. As a result, many obligations that are more serious for CSPs were introduced, such as conducting risk assessments, ensuring proper breach reporting, and adopting comprehensive cybersecurity measures.[47] Moreover, it highlights the necessity of supply chain security.[48] Pointing out that any faults or shortcomings in third-party suppliers can limit the authenticity of cloud providers. Therefore, CSPs have to ensure that during the whole supply chain the data go through; there is risk evaluation done appropriately by promoting accountability and resilience covering all parts of its ecosystem as well as ensuring security measures extend beyond their infrastructure. This is very beneficial since it is common to deploy intricate networks of third-party suppliers and subcontractors in the cloud.[49] To

[44] Niels Vandezande: Cybersecurity in the EU: how the NIS2- Directive stacks up against its predecessor. 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4383118 (Accessed: 13/1/2025).

[45] Articles 5, 7, 18 of the NIS2.

[46] Articles 2, 3 of the NIS2.

[47] W. Kuan Hon: Cloud Service Providers under the NIS Directive – the UK's implementation (with GDPR comparisons). 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3200149 (Accessed: 15/1/2025).

[48] Article 21 paragraph (2) of the NIS2.

[49] Vandezande 2023, Ibid.

promote cooperation among CSPs and other stakeholders like public authorities, for example, the NIS2 explained related issues such as incident reporting and effective information-sharing mechanisms.[50] Targeting to minimize the side effects of cybersecurity breaches to guarantee continuous services and increase trust in cloud computing environments.[51]

The NIS2 directive is pivotal legislation for a secure cloud environment. It contributes to reducing risks, increasing trust, and helping to achieve a resilient cloud environment. However, some challenges and obstacles may occur by applying its provisions. The guarantee that its application of the same standards to achieve security in the cloud environment among all member states of the Union, which constitutes one of the most important goals of this directive, may be the primary challenge, as application practices differ from one member state to another. Moreover, it is very complex to maintain security throughout the supply chain in the cloud since they usually rely on a diverse network of multiple third-party services, and ensuring strong and sufficient security within all of that while keeping high levels of innovation could constitute a serious hindrance. Lastly, the incident reporting provisions may harm the institution's reputation, thus, cloud service companies may think twice before reporting any breaches, considering the effects of losing clients' trust. Therefore, reaching a balance between transparency and ensuring trust continuously is a critical aspect to focus on.

6. Digital Services Act (DSA) and Digital Markets Act (DMA)

The (DSA) and (DMA) are two key pieces of legislation that came with significant provisions covering and regulating the broader digital ecosystem. In the cloud environment, issues like CSPs as a hosting service, platform services obligations, data protection, and competition in the digital market are mainly addressed by the above-mentioned acts, along with other relevant rules that we will look at in the following.

When it comes to digital safety, the DSA is a vital legislation with its main scope focusing on the organization of the online platforms in a way that provides sufficient safety for users, stipulating the legal obligations and liabilities of the service providers or "platform providers". Therefore, CSPs as platform providers fall within the obligations of this act. Mainly when running under the PAAS deployment model among the three models in general. Liability and accountability

[50] Articles 21 and Article 23 of the NIS2.
[51] Hon 2018, Ibid.

are two focuses of the DSA. CSPs are responsible for the user's data or the third party's data they host or distribute as platform service providers. They are liable for the safety of this data stored by a user. However, under certain circumstances, they could be exempt from such liability. Terms and conditions transparency got precise care from the DSA. CSPs as intermediary service providers, according to this act, are accountable for providing any necessary details for any restrictions[52] connected to the services they provide in their terms and conditions statement. Moreover, it is highly important in this regard to ensure that these terms and conditions are explicit and written in simple, clear words with the misuse or the illegal action. It can be seen as a big challenge practically since these wide-meaning terms may differ from one country to another. Similarly, they may hold a much more complex meaning when applied to various scenarios.

Special organization of large platforms introduced by the DSA, establishing a specific framework for big service providers. Usually, CSPs are classified as big service providers, which comes from the nature of their function. Thus, they must adhere to the DSA provisions in this regard.[53] It is to be noted that these articles impose stricter obligations on VLOPs. Consequently, CSPs are under a rigorous framework for compliance purposes. The DSA came with several effective content that have had a significant impact, mainly on promoting consumer protection in the cloud and organizing big CSPs. However, by reviewing this act, we can notice that it may place numerous challenges to its application on the CSPs. Most importantly, those provisions related to the modification of data content, which are in a potential conflict with GDPR in this regard, mainly for principles such as lawfulness, fairness, transparency, data minimization, purpose limitation, and user consent. Finally, yet importantly, such strict obligations may hurt the development of the cloud industry, additionally, it may prevent smaller competitors and evolving startups from entering the market.

Complementarily, the DMA brought several requirements for digital service providers, primary obligations and prohibitions that would enhance the security and safety of personal data in the cloud and protect competition in the digital market. Further provisions were added regarding big CSPs under the DMA. They could be classified as Gatekeepers if they meet specific requirements.[54] Which consequently puts more obligations on CSPs acting under this condition.

A key provision of the Digital Markets Act (DMA) is the restriction on Cloud Service Providers (CSPs) from processing personal data for online advertising

[52] A good example to give for this is an illegal activity.
[53] Article 33 of the DSA.
[54] Article 3 paragraph (1) of the DMA.

without obtaining prior legal consent from the data subject.[55] This provision not only enhances data security in the cloud but also addresses the critical issue of data ownership, a controversial legal concern in cloud data protection. By requiring user consent for online ads, the DMA strengthens user control over their data. Additionally, when CSPs offer multiple services, the DMA prohibits combining data across services or using it for other purposes, particularly when CSPs act as gatekeepers. Gatekeepers are also restricted from signing end users into additional services or combining personal data without consent.

The DMA further promotes data portability and interoperability, ensuring that consumers can transfer their data to third-party services without discrimination or unjust restrictions by gatekeepers. These measures aim to prevent anti-competitive behavior and protect consumer choice, reinforcing the DMA's goal of fostering fair competition in the digital market.

This act provides wide and comprehensive obligations and prohibitions which, by applying in the cloud market, would ensure fair competition and transparency, leading to provide cloud services by the gatekeeper in a form free of illegal restrictions.

7. Cybersecurity Act and ENISA

In June 2019, a significant step was taken to enrich the security and resilience of the digital market by adapting the (CSA). Its goal is mainly to highlight the role of the European Agency for Cybersecurity and the establishment of the EU cybersecurity certification schemes (CSA).[56]

The CSA came with various obligations and suggested exceptional requirements useful to adapt by the CSPs to ensure compliance and upgrade confidence among customers. The foundation of the cybersecurity certification framework by the act would help CSPs to achieve the best compliance and security for the data. This approach proposed by the CSA aimed to approve that the ICT products, services, and processes undergo specific security measures to guarantee reliability, trust, compliance, and security throughout the lifecycle of the data in the cloud.[57] Certification schemes, also known as conformity assessment, *"a demonstration that specified requirements are met which usually includes (activities such as testing, inspection, validation, verification, certification, and accreditation). Specified requirement – a need or expectation that is specified (the specified requirements can be stated in*

[55] Article 5 paragraph (2) point a) of the DMA.
[56] Article 1 of the CSA.
[57] Article 46 of the CSA.

regulatory documents such as regulations, standards, and technical specifications. The specified requirements can be detailed and general)".[58] The certification scheme has several security objectives that are relatively crucial for building a secure cloud ecosystem. By the nature of the cloud, a huge amount of data is processed, stored, and transmitted. One of the most important goals of the CSA is to prevent any unauthorized access, storage, disclosure, or destruction of affected data. Such access is only permitted by authorized persons, programs, or machines.[59]

The CSA grants the European Union Agency for Cybersecurity (ENISA) the leading role in implementing and controlling these certification mechanisms. Together with the European Commission, ENISA and national authorities in the EU shall organize the certification schemes, considering relevant legislation such as the GDPR, NIS2, and others.[60] Certification schemes would increase the trust of the CSP's customers by showing official certificates of legal security measures taken to ensure the best compliance. However, the certification under Article 46 of the (DMA) presents several challenges. First, since certification is voluntary, some Cloud Service Providers (CSPs) may choose not to comply, potentially undermining customer trust. Second, non-EU CSPs may encounter difficulties in meeting EU certification requirements, and EU certifications may face recognition issues in foreign jurisdictions, particularly concerning cross-border data transfers. Third, compliance with the certification requirements may impose significant costs, especially on smaller CSPs, due to the ongoing obligations for certified services. Although the certification aims to demonstrate continuous compliance, CSPs remain responsible for legal breaches, which could create legal uncertainties for customers.[61] Finally, the certification scheme primarily addresses security but does not cover privacy concerns, such as those outlined in the GDPR, leaving a gap in the broader regulatory framework.

8. Conclusion

This review examines key EU regulations affecting cloud technology: the GDPR, NIS2 Directive, DSA & DMA, and the Cybersecurity Act, which collectively establish compliance standards for data protection, security, privacy, fair competition, and data subject rights in the cloud. The GDPR addresses data privacy

[58] Olena Tsvilii: Cyber Security Regulation. Cyber Security Certification of Operational Technologies. *Technology audit and production reserves*, 2021 (1), https://ssrn.com/abstract=3796990.

[59] Article 51 point c) of the CSA.

[60] Article 52 of the CSA.

[61] Article 54 of the CSA.

and cross-border data transfers, with CSPs typically acting as data processors and users as data controllers, though ambiguities in roles and liabilities may arise, especially in multi-service cloud models. The DSA and DMA improve accountability and fair competition but impose stricter obligations on CSPs acting as gatekeepers, which could disadvantage smaller players. The Cybersecurity Act supports trust through voluntary cybersecurity certification schemes, while NIS2 emphasizes supply chain security, incident reporting, and risk assessments for secure cloud operations. Despite these efforts, achieving consistent, high compliance across the EU remains a significant challenge.

To improve the regulatory framework of the cloud technology in the EU, we recommend that the roles and responsibilities of the cloud actors should be clarified precisely, taking into account the GDPR provisions. CSPs should provide tools for cloud users to manage their data security and cross-border compliance. Also, certification schemes under the CSA should be mandatory in sensitive data, at least in the healthcare and finance sectors. Importantly, financial support should be provided for small CSPs for fair competition, and at least to make the certification costs shared between the providers and users. Lastly, to reinforce data security, transparency, and accountability in the cloud, the integration of Blockchain technology is an advised step. It would contribute to reducing the risks of data breaches, ensuring data integrity, and promoting trust among cloud users. Therefore, it is highly recommended that CSPs implement these technology features and techniques to achieve the best security compliance.

Bibliography

Literature

Giulio D'Agostino: *Data security in cloud computing volume*. Vol. I. New York, Momentum Press, 2019.

Preston De Guise: *Data protection: Ensuring data availability*. London, CRC press, 2020.

Theo Lynn – John G. Mooney et al.: *Data Privacy and Trust in Cloud Computing*. Palgrave Macmillan, 2021.

Kevin McGillivray: *Government Cloud Procurement*. Cambridge University Press, 2022.

Christopher Millard: *Cloud Computing Law*. Oxford University Press, 2021.

Vineeth Narayanan: Harnessing the cloud: international law implications of cloud computing. *Chicago Journal of International Law*, 2012 (2).

Joe Weinman: *Cloudonomics. The business value of cloud computing*. John Wiley & Sons, 2012.

Online sources

'Europe Cloud Computing Market Size' (Mordor Intelligence, Online Report), https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market (Accessed 23 January 2025).

'Market Trends of Europe Cloud Computing Industry' (Mordor Intelligence, Online Report) https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market/market-trends (Accessed 20 January 2025).

W. Kuan Hon: Cloud Service Providers under the NIS Directive – the UK's implementation (with GDPR comparisons). 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3200149 (Accessed: 15/1/2025).

Richard G. Lipsey – Kenneth I. Carlaw: *Economic transformations: general-purpose technologies and long-term economic growth*. Oxford University Press, 2005, https://www.researchgate.net/publication/227468040_Economic_Transformations_General_Purpose_Technologies_and_Long-Term_Economic_Growth (Accessed: 22/12/2024).

Olena Tsvilii: Cyber Security Regulation. Cyber Security Certification of Operational Technologies. *Technology audit and production reserves*, 2021 (1), https://ssrn.com/abstract=3796990.

Niels Vandezande: Cybersecurity in the EU: how the NIS2- Directive stacks up against its predecessor. 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4383118 (Accessed: 13/1/2025).

Legislations

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation).

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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 and repealing Directive 95/46/EC (NIS2 Directive).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act).

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 (Digital Markets Act).

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