The potential effects of recent EU cybersecurity and resilience regulations on cloud adoption and EU cyber resilience

Guy WAIZEL*

Abstract

This paper delves into the potential impacts of the recently published Network and Information Security Directive 2 (NIS2) and Digital Operational Resilience Act (DORA) on EU cybersecurity resilience and cloud adoption. Employing a mixed method of descriptive literature review, narrative review, and thematic synthesis, we explore challenges for implementation, drawing from past data privacy regulations, notably the GDPR, which served as a basis for our analysis and has already significantly affected many organizations. We emphasize the need for efficient software solutions to assist organizations in complying with the new regulations, building upon lessons learned from the GDPR. Cloud service providers and enterprise software vendors are identified as key players to address these challenges. This paper discusses the paradox of organizations' historical reluctance to migrate to the cloud due to data privacy concerns, and how the motivation to comply with recent regulations may now drive increased modern cloud adoption.

Keywords: DORA, NIS2, data privacy, cybersecurity, resilience

Introduction

This paper aims to identify the potential effect of NIS2 and DORA on modern cloud adoption among various organizations that will need to comply with the regulations, examine the effect on overall resilience in the EU, and serve as an initial wake-up call for organizations that will need to comply with these new regulations.

The NIS2 (Network and Information Systems) Directive (EU) 2022/2555 from December 2022 replaces and expands the original EU NIS Directive. It uses legal measures to improve cybersecurity throughout the EU by defining critical sectors based on size. The new directive places greater focus on cybersecurity efficiency and addressing supply chain threats, defining supervisory measures, developing better cooperation between member states regarding sanctions, and increasing threat and information-sharing opportunities. EU member states were requested to publish all measures required for organizations to comply with the NIS2 Directive by October 2024 (Directive (EU) 2022/2555, 2022; NIS 2 Directive, 2023).

* Guy WAIZEL is researcher at Alexandru Ioan Cuza University of Iasi, Romania, e-mail: guy.waizel@gmail.com.

The Digital Operation Resilience Act (DORA) EU 2022/2554 is an EU regulation that will become applicable from January 2025, and will affect the entire financial sector and vendors' development roadmaps. Financial institutions must comply with new risk management rules for information and communication technology (ICT), such as incident reporting, resilience testing, and ICT third-party risk monitoring. Organizations will need to reassess their contractual relationships with vendors (Digital Operational Resilience Act (Regulation (EU) 2022/2554, 2022; DORA, 2023).

Many challenges are expected to arise when NIS2 and DORA roll into official laws in individual member states. Organizations are encouraged to use the time allocated wisely by checking the implications, improving their processes, and applying changes and adjustments accordingly.

To address the critical gap in understanding how the NIS2 and DORA regulations will impact cloud adoption and cybersecurity resilience in the EU, our research leverages insights gained from past data privacy regulations, particularly the GDPR. This approach provides clarity on the potential implications of these new directives, answering the central question of how these regulations and other future data privacy regulations will shape the landscape of modern cloud adoption and overall cyber resilience in the EU. Our meticulous descriptive literature review and narrative synthesis analysis of fifty-five articles allow us to identify common trends, themes, and key findings that elucidate both the positive and negative effects of NIS2 and DORA on cybersecurity and resilience in the EU in the coming years.

1. Literature review - the GDPR effect on organizations

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, 2018) dramatically changed how business organizations treat and protect their data. In the context of cybersecurity and resilience, the GDPR served as a catalyst for organizations globally to reevaluate their data management practices and enhance their cyber resilience strategies. Organizations underwent a comprehensive overhaul of global business processes and workflows, with a keen focus on mapping risks within databases to address potential GDPR violations urgently and effectively.

Marketing campaign strategies, sales activities, and organizational processes underwent significant transformations to align with the new GDPR requirements. This shift included adapting product development to incorporate GDPR support, ensuring corporate websites met compliance standards. Johnson *et al*., (2023) highlighted the immediate impact, noting a 15% overall decrease in the use of web technology vendors in the week following GDPR enforcement. Additionally, popular vendors experienced a 17% increase in market concentration, reflecting user preference for trusted, compliant vendors.

Despite these efforts, organizations encountered challenges, with some perceiving a slowdown in business growth and development due to GDPR compliance. Chazan (2017) discussed SAP's concerns about potential adverse effects on startups because of the stringent regulations. This literature emphasizes that the GDPR not only shaped data protection practices but also influenced broader organizational strategies, setting the stage for understanding the potential impact of subsequent regulations on cybersecurity and cloud adoption.

While many organizations endeavored to comply, some fell short, leading to breaches and fines. Ford *et al*. (2021) demonstrated that a company's market value could decrease following a publicly announced GDPR fine, highlighting the financial consequences of non-compliance.

2. Literature review - the GDPR effect on cloud service providers

Taylor (2011) predicted that cloud providers would incorporate more geographic location features to support data sovereignty in 2011, a forecast realized through Data Citizenship and Complaint Data Transfer using location tags. This anticipation of data sovereignty concerns aligns with the GDPR's emphasis on data protection, leading cloud service providers to implement features in 2018 supporting GDPR compliance. Cloud giants such as Google, Amazon, Oracle, and Microsoft, as detailed by Spasic *et al*. (2019), introduced solutions like AWS and Azure that not only adhered to GDPR requirements but also demonstrated the proactive steps taken by cloud providers to ensure data security and compliance (Figure 1). This underlines the interconnected relationship between data protection regulations, cloud service providers, and the broader cybersecurity landscape.

Google Cloud Platform (GCP) underlines its commitment to supporting GDPR (Google, 2023a), and Oracle details its GDPR support on its website (Oracle, 2023). In response to GDPR and other data privacy regulations, studies delve into technical implementation technologies and algorithmic solutions. Corliss, M. (2010) proposed the need for a balance between technology and data privacy regulations to expedite compliance, emphasizing a harmonious integration of both elements. Ko, S. Y. *et al*. (2011) advocated for the HyberEX model in 2011, specifically designed for enhancing privacy in cloud environments. Raghavan *et al*. (2021) highlighted the role of De-Identification of Personal Information (DIPI) technology in safeguarding data privacy within big data applications in Asia.

Figure 1. Solutions of AWS and Azure for GDPR requirements

Category	Pattern title	Solutions in AWS	Solutions in Azure
Compliance and Regulatory	**Data Citizenship**	Use AWS location tags to designate the location for data processing	Azure information protection and location tag. Azure frontdoor service
	Cryptographic Erasure	Use AWS KMS	Use Azure Key Vault
	Shared Responsibility Model	AWS provides different services to ensure protection of data and system. It is upto client to use it or not. However, AWS is responsible for only the vailability and basic security of cloud platform.	Azure provides different security tools to ensure protection of data and system. It is upto client to use it or not. However, Azure is responsible for only the vailability and basic security of cloud platform
	Compliant Data Transfer	AWS locaton tags	Azure location tag
	Data Retention	The data retention policies can be defined and executed by AWS. For example Lambda	Azure provides option to define data retention policy in Database system
	Data Lifecycle	AWS data lifecycle manager	Azure blob storage lifecycle
	Intentional Data Remanence	database (e.g. DynamoDB)	database (e.g. Azure backup)
Identification, Authentication and Authorisation	**Multi-Factor Authentication**	AWS Cognito	Azure active directory : multi-factor
	Federation (Single Sign-On)	AWS SSO (Single Sign-On)	Azure AD Seamless Single Sign-On
	Access Token	AWS security token service	Azure active directory : Token service
	Mutual Authentication	Use AWS TLS/SSL certificate, Certificate feature of API Gateway (AWS client VPN)	Azure App service
	Secure User Onboarding	AWS customer on boarding	Azure security center
	Identity and Access Manager	AWS IAM and Cognito	Azure IAM
	Per-request Authentication	AWS Signing and Authenticating REST Requests	Azure API management & REST API authentication
	Access Control Clearance	AWS cloud watch and AWS Cognito/IAM	Azure access control service
Secure Development, Operation and Administration	**Bastion Server**	AWS bastion host	Azure Bastion host
	Automated Threat Detection	AWS GuardDuty	Azure advanced threat protection
	Durable Availability	AWS cloud watch, AWS WAF	Azure web access firewall & firewall application gateway
	Economic Durability	AWS cloud watch	Azure Monitor
	Vulnerability Management	AWS vulnerability scanning	Vulnerability scan in Azure security center
Privacy and Confidentiality	**End-to-End Security**	AWS KMS, Certificate manager	Azure Key Vault
	Computation on Encrypted Data	N/A	N/A
	Data Anonymisation	Algorithms can be defined and ran by AWS module (e.g. lambda)	Azure provides Dynamic Data Masking on SQL database
	Processing Purpose Control	N/A	N/A
Secure Architecture	**Virtual Network**	AWS Virtual Private Cloud	Azure Virtual Network
	Web Application Firewall	AWS WAF	Azure application firewall gateway
	Secure Element	AWS IoT Device Management	Azure IoT Hub & IoT Suit
	Secure Cold Storage	AWS Glacier	Azure Coldblob storage
	Certificate and Key Manager	AWS Certificate and Key manager (AWS KMS)	Azure Key Vault
	Hardware Security Module	AWS CloudHSM	Azure Dedicated HSM
	Secure Auditing	AWS Auditing Security Checklist	Azure Monitor, Stream, Network Watcher

Source: Spasic *et al.*, 2019

Georgiou and Lambrinoudakis (2020) presented insights into modifying cloud security policies to support GDPR, providing valuable guidance for developers, particularly in the context of cloud-based healthcare systems. Glova (2022) suggested various algorithmic approaches to secure and privacy-preserving computation in data centers, emphasizing the ongoing quest for robust privacy solutions. Jain *et al*. (2016) addressed challenges in existing data-privacy implementations like HybrEx, k-anonymity, T-closeness, and L-diversity. The need for more recent privacy-preservation

mechanisms in big data, such as hiding a needle in a haystack, identity-based anonymization, differential privacy, privacy-preserving big data publishing, and fast anonymization of big data streams, was advocated by Jain. Alnajrani and Norman (2020) derived seven hypotheses supporting the utilization of the privacy by design model (PbD) in mobile cloud computing (MCC) for privacy preservation.

Cloud service providers and enterprise vendors play a crucial role in offering advanced features to meet GDPR requirements. As highlighted by Spasic *et al*. (2019), organizations leverage these offerings to save time and effort, avoiding the need for unique on-premises customization and configurations to meet the regulations. This underscores the symbiotic relationship between regulatory compliance, technological innovation, and the support provided by cloud service providers in the evolving landscape of data protection.

3. Methods

For this paper, a deliberately chosen mixed method of descriptive literature review (King and He, 2005; Pare *et al*., 2015; Petersen *et al*., 2015) and narrative review (Cronin *et al*., 2008; Green *et al*., 2006; Levy and Ellis, 2006; Webster and Watson, 2002) was conducted. Qualitative techniques of content analysis, narrative analysis, and thematic synthesis were employed. A strategic analysis covered journals, theses, and research papers from four databases: Google Scholar, Proquest, Science Open, and Base-search.net. The primary objective was to identify patterns and gaps in the literature, focusing on known findings, theories, and concepts. To achieve this, the sources were mapped, evaluated, and subjected to content analysis to uncover patterns and relationships. This robust approach aimed to enhance the depth and breadth of insights gained from the literature, aligning with the comprehensive nature of the study.

For the descriptive review, the following steps were employed: Initial search within the databases, identifying and exploring literature focusing on the topic, evaluation, and analysis, piling the literature by main concept categories, organizing information in a table, and sorting key findings. These steps were chosen to systematically extract relevant information, provide a structured analysis, and ensure a comprehensive coverage of the literature landscape. Mixed techniques, including an inductive approach using content analysis to explore main themes and a deductive approach to uncover trends and connections, were utilized by interpreting common keyword frequencies from the abstracts of every article. The inductive approach allowed for an open exploration of emerging themes, while the deductive approach facilitated the identification of overarching trends and connections, adding depth and context to the analysis.

The results were then synthesized using thematic narrative synthesis, drawing common findings and insights and suggesting potential implications for future research. The descriptive review tabling structure is described in Table 1. The search keywords used included the following words and phrases: "NIS2 Directive"; "DORA regulation"; "DORA Act"; "EU recent regulations (2020-2023)"; "effect of NIS2 and DORA on cloud adoption"; "effect of NIS2 and DORA on cybersecurity and resilience"; "data privacy and cloud adoption"; "GDPR effects"; "data privacy regulations(2011+)"; "Directive(EU)2022/2555"; "Regulation (EU)2022/2554"; "digital operational resilience for the financial sector".

The criteria for inclusion in the literature review were: Most relevant to the article's topic and disciplines; article types: scholarly journal, books, dissertations and theses, and papers in response to the latest regulations announcements.

Table 1. Descriptive literature review tabling

Article Title	Author & Published Year	Main Theme	Aim	Conclusion	Common Findings/Gaps and Relation to the Topic	Disciplines	Reference

Content analysis technique was used: abstracts of articles were coded; main themes were identified using WordCloud: trends, insights, patterns and relationships were uncovered; and narrative thematic synthesis was conducted to gather conclusions. This detailed and multi-faceted approach ensured a nuanced understanding of the literature, capturing not only the main themes but also the subtleties and interconnections within the data. The methodology exhibits strengths in comprehensive coverage through the inclusion of diverse databases and literature sources, fostering a thorough understanding of the topic. Additionally, the use of mixed methods, combining descriptive literature review and narrative review techniques, enables a multifaceted exploration of the research landscape. However, weaknesses include the potential introduction of subjectivity in qualitative data interpretation and the limited generalizability of findings due to specific search criteria and a focus on recent regulations.

4. Results

4.1. Identified themes

The initial search results yielded over one hundred and sixty articles, reflecting the breadth of literature on the subject. The rigorously applied inclusion criteria, detailed in the methodology, were

pivotal in selecting articles that adhered to specific parameters. Fifty-five articles successfully met these inclusion criteria, demonstrating their alignment with the research focus on recent EU cybersecurity and resilience regulations, specifically the NIS2 Directive and DORA. These inclusion criteria ensured a targeted selection, emphasizing relevance and direct applicability to the study's objectives.

Subsequently, the selected articles underwent a meticulous analysis, utilizing qualitative techniques such as content analysis and thematic synthesis. This process not only affirmed the relevance of the chosen articles but also led to the identification of four overarching themes, as elucidated in Table 2. These themes comprehensively covered various aspects of the literature, including challenges in the adoption of data privacy regulations, consequences such as fines following infringements, responses and actions taken in the context of data privacy regulations, and considerations specific to data privacy regulations within cloud environments, encompassing methods to preserve privacy. This systematic approach ensured a nuanced exploration of the literature, enriching the depth of insights derived from the selected articles.

As a concise summary, Table 3 serves as a visual representation of the literature review, classifying the findings based on the identified themes. This categorization not only aids in organizing and presenting the results but also provides a structured reference point for readers to navigate through the diverse dimensions of the literature. The inclusion criteria, implemented with precision, were instrumental in refining the article selection, guaranteeing that the chosen literature directly contributed to the elucidation and exploration of pivotal themes, thereby enhancing the overall depth and relevance of the descriptive literature review.

Table 2. Identified themes

Theme	Theme's Reference	Year
1. Challenges in adopting data privacy regulations	Barbara, C. G. *et al.*	2001
	Nauwelaerts, W	2004
	Taylor, P	2011
	Chazan, G	2017
	Cutler, S	2018
	Ross, W	2018
	Newstex	2019
	Bartlett, T	2020
	Tzanou, M	2020
	Jacuch, A., PhD	2021
	Perdereaux-Weekes, A	2021
	Biasin, E., and Kamenjasevic, E	2022
2. Fines following infringement of data privacy regulations	Murgia, M., and Coulter, M.	2019
	Ford, A *et al.*	2021
	Venkataramakrishnan, S	2021

3. Responses and actions related to data privacy regulations	EBA	2019
	Copeland, L., Jr	2021
	EIOPA	2020
	ESMA	2020
	ITI	2021
	NIS2	2021
	Rajamäki, J	2021
	ITI	2021
	Targeted News Service, Washington, D.C	2021
	Schmitz-Berndt, S., and Chiara, P. G	2022
	Splunk	2022
	Targeted News Service, Washington, D.C	2022
	DORA	2022
	GDPR	2023
	Google	2023a,2023b,2023c
	MENA Report, London: SyndiGate Media Inc	2023
	Microsoft	2023a,2023b
4. Data privacy regulations in the cloud and preserving privacy methods	Machanavajjhala,A. *et al.*	2007
	Corliss, M	2010
	Ko, S. Y. *et al.*	2011
	Domingo-Ferrer, J., and Soria-Comas, J	2015
	Jain, P., Gyanchandani,M., and Khare, N	2016
	Express Computer, Mumbai	2018
	Singh, N., and Singh, A. K	2018
	CommunicationsToday, Noida	2019
	Spasic, B. *et al.*	2019
	Alnajrani, H. M., and Norman, A. A	2020
	Georgiou, D., and Lambrinoudakis	2020
	Mahanan, W. *et al.*	2021
	Raghavan, A. *et al.*	2021
	Amiri-Zarandi. *et al.*	2022
	Glova, A. O	2022
	Gartner	2023
	Google	2023a,2023b,2023c
	Johnson, G. *et al.*	2023

Table 3. Summary of literature review and themes classification

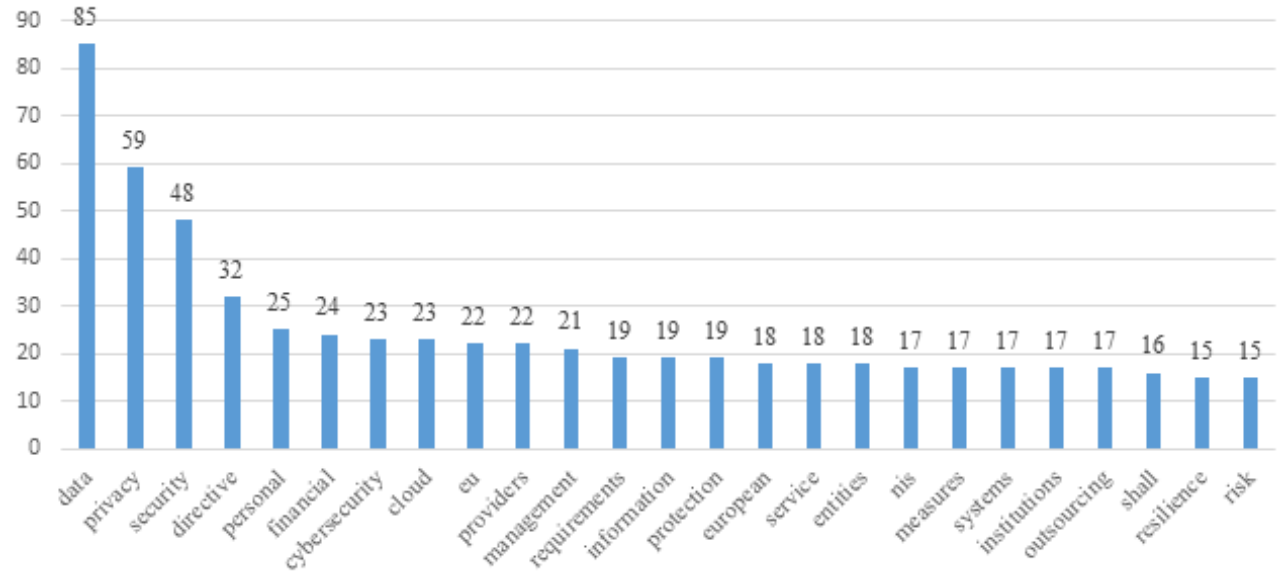
Theme	**Count of Articles**
Challenges in adopting data privacy regulations	12
Fines following infringement of data privacy regulations	3
Responses and actions related to data privacy regulations	20
Data privacy regulations in the cloud and preserving privacy methods	20

Using the WordCloud app (Free Word Cloud Generator, 2023), the word frequency of all article abstracts was analyzed. Most of the articles do not contain the words DORA and NIS2, which implies insufficient literature and a knowledge gap about the effect of these regulations, challenges and barriers, and other implications (Figure 2). This reinforces the importance of this article's contribution to the literature in refining the barriers, the gaps, and the potential effects of these regulations.

The top fifty keywords identified in the frequency analysis are words that are linked with the topic and widely discussed in the literature, such as data privacy, cybersecurity, directive, personal, financial, and cloud. Among the top ten keywords were cloud and cybersecurity, suggesting a strong relationship with the topic of these regulations. However, the analysis did not reveal a specific relationship between cloud adoption and data privacy regulation, and resilience only ranked 24th. This finding highlights the need for further research on these two topics, such as this study (Figure 3).

Figure 2. Top 50 keywords in the article abstracts

Figure 3. Abstracts word frequency



4.2. Narrative analysis and thematic synthesis

Through a comprehensive narrative analysis and thematic synthesis of fifty-five papers, including journals, theses, and various research articles connected to data privacy, cloud adoption, and cyber resilience, encompassing both qualitative and quantitative papers that meet the inclusion criteria and align with the keyword search used, this study aims to provide an in-depth understanding of the effect of NIS2 and DORA on cloud adoption and the potential implications for cybersecurity and resilience in the EU. The following are the conclusions drawn from the thematic synthesis:

Balance is required between data privacy regulations and technology adoption (Corliss, M., 2010) and most of the world population will be covered under modern data privacy regulations by 2024 (Gartner, 2023).

New data privacy preservations algorithms methods and technologies are making it easier to implement regulations over the cloud and big data applications. (Alnajrani and Norman, 2020; Amiri-Zarandi *et al.*, 2022; Communications Today, 2019; Express Computer, 2018; Corliss, 2010; Domingo-Ferrer and Soria-Comas, 2015; Georgiou and Lambrinoudakis, 2020; Glova, 2022; Gartner, 2023; Google 2023a, 2023b; Johnson *et al*., 2023; Jain, Gyanchandani and Khare, 2016; Ko *et al.*, 2011; Machanavajjhala *et al*., 2007; Mahanan *et al*., 2021; Raghavan *et al*., 2021; Singh and Singh, 2018; Spasic, 2019). Data privacy on the cloud is covered extensively in literature by cloud service providers. For example: (Google 2023a, 2023b, 2023c; Microsoft, 2023a; 2023b; Oracle, 2023; Spasic, B *et al.* ,2019). Microsoft already submitted a list of recommendations in response to the NIS2 regulation (Microsoft, 2023b). Google claim that in many aspects, security on the cloud exceeds on-premises security (Google, 2023b).

IoT vendors must address data privacy by design (PbD) and development, for items such as medical devices, smart city sensors, and CCTV surveillance that are used to collect data. When PbD was utilized, it improved privacy (Alnajrani and Norman, 2020; Biasin and Kamenjašević, 2022). Designing and developing products to include protection and meet the requirements for NIS2 and DORA will take time. Hackers and nation-state actors can leverage the time between legislation and implementation, take advantage of existing vulnerable IoT devices, and use this time gap for extensive attacks.

New directives will have a significant effect outside of the EU. For example, if a US global organization has branches in EU, they should get prepared and check the implications; during M&A processes, regulations need to be followed. It also needs to be considered regarding data requests from courts. For example, Nauwelaerts (2004) pointed out the importance of meeting with data privacy regulations even during the negotiation of the M&A, especially if the buyer is a US entity

and the seller has European employees, and Barbara *et al.* (2001) raised the challenges US and other companies have in complying with EU regulations. Cutler (2018) discusses the effect of EU data privacy regulations in US courts; for example, when a court orders data to be produced which is protected by EU data privacy regulation, The court may consider using Hague evidence convention. In the new regulations, penalties are defined between a fixed amount to a percentage of the organization's global annual turnover. The higher of the two amounts will be imposed on large global organizations, so although the effect may seem to be only on EU member states it is already clear that global organizations will also be affected.

Fines, sanctions, and enforcement are expected to rise as soon as legislation is passed in member states and becomes effective. Since the number of sectors has increased, organizations with more than 250 employees which meet the defined criteria of essential or important entities will be included (NIS2, 2023; Directive (EU) 2022/2555, 2022). More enforcement and fines are expected, especially after cyber breach incidents and the failure of organizations to protect their data. It was also the case after enforcing GDPR and other past regulations. For example, the following papers discuss penalties for organizations following the infringement of GDPR: (Ford *et al.*, 2021; Murgia and Coulter, 2019; Venkataramakrishnan, 2021).

The public is not sufficiently concerned about the broad exposure of vulnerabilities of IoT devices (Bartlett, T, 2020). Based on historical studies, data privacy regulations may slow down startups and new organizational developments (Chazan, 2017; Taylor, 2011; Ross, 2018). Some EU member states would need to invest much more than others to prepare since their level of resilience and cybersecurity is not as advanced as other states (Jacuch, 2021; MENA Report, 2023; Rajamäki, 2021). Additionally, some member states face an increased risk of attacks compared to others. For example, specific member states that face significant attacks were identified in the recent threat report by Trellix (Trellix, 2023).

Organizations in the EU will need to allocate more funding for resilience and cybersecurity products and cloud service providers to prepare for the new EU regulations and equip themselves with new enhanced features to assist in complying with the regulations. In recent years, EU member states invested much less than the US in cybersecurity, and so the upcoming budg*et al*located by the EU to cybersecurity has been raised (NIS2, 2023; Directive (EU) 2022/2555, 2022).

EU organizations above 250 employees meeting the defined criteria of essential or important entity should work fast to identify and explore the most appropriate cybersecurity software, data protection resilience software, and technology tools that can support their efforts to comply rapidly with the requirements of the new regulations.

Cooperation between member states is required for intelligence sharing. Member states would need to expand their joint knowledgebases, vulnerability disclosure, and processes for escalations at all levels (Directive (EU) 2022/2555,2022; Dora, 2023; NIS2, 2023; Regulation (EU) 2022/2554, 2022).

Ransomware attacks, advanced persistent threats (APT), and supply chain attacks are expected to grow. Based on a Trellix report from 2022, 38% of global ransomware family attacks hit EU countries (Directive (EU) 2022/2555,2022; NIS2, 2023; Trellix, 2022).

Organizations would need to seek and assess tools to improve their early warning detection capabilities and resilience programs by ensuring proper backup and recovery, and business contingency plans covering and protecting data across all platforms used within their organization. They should improve mitigation, remediation, and containment capabilities. Organizations would need early detection solutions to meet the requirements of reporting significant attacks within seventy-two hours (Directive (EU) 2022/2555,2022; NIS2, 2023). Early detection systems, such as systems based on active defense technology and deception technology, may act as a game changers when trying to keep up with tight Service Level Agreement (SLA) reporting of detection. Organizations need to improve their resilience by ensuring they can easily protect web services and workloads, and restore systems backups within a specified recovery point objective (RPO) and recovery time objective (RTO). They should ensure resilience with their cloud assets such as cloud mailbox, workloads, instances, virtual machines, databases, containers, and blobs buckets. They should ensure proper retention backup to meet sovereignty requirements by using regions, proper retention, and new features to comply more effectively with the regulations.

Technologies and solutions to assist in complying with early warning, detection, and business contingency would significantly help organizations meet their needs. For example, the following articles in Directive (EU) 2022/2555 (Directive (EU) 2022/2555, 2022) support it:

- Article 21, “Cybersecurity risk-management measures,” refers to business continuity, such as backup management and disaster recovery, crisis management, supply chain security, and security in networks, which encompasses threat detection in networks.
- Article 11 and article 15 “Computer Security Incident Response Team (CSIRT) Network requirements, technical capabilities, and tasks of CSIRTs” refer to early warning detection.
- Article 23, “Reporting obligations” refers to early warning detection.
- Article 29 “Cybersecurity information-sharing arrangements” refers to detection capabilities. In the Regulation (EU) 2022/2554 (DORA regulation, 2022; Regulation (EU) 2022/2554,2022).

- Article 10 refers to detection capabilities.
- Article 11 refers to response and recovery and backup.
- Article 12 refers to backup policies and procedures, restoration and recovery procedures, and methods.
- Article 15 refers to further "harmonization of ICT risk management tools, methods, processes and policies" which encompasses detection capabilities.
- Article 17, "ICT-related incident management process" refers to early warning detection.
- Article 45, "Information-sharing arrangements on cyber threat information and intelligence," refers to threat detection.

The regulation emphasizes the importance of cooperation between member states and intelligence sharing. New software offerings for cybersecurity intelligence sharing capabilities between EU member states for incident reporting and vulnerability disclosure are an opportunity ripe for development by enterprise software vendors.

Contractors' terms and contracts will need to be reevaluated and assessed by the legal teams of both vendors and customers, with care taken to protect both sides from unexpected fines (Directive (EU) 2022/2555, 2022; DORA, 2023; NIS2, 2023; Regulation (EU) 2022/2554, 2022). Contracts specifying new obligations and responsibilities will need to be modified to meet the requirements. Vendors may face increased exposure to chain trials where the government may fine an organization and the organization in turn sues its vendor for not complying with new policies. Supply chain mapping and assessment will need to examine every vendor in the chain to ensure mapping was done correctly and that no vendor contract is missing. Organizations will need to invest more in data privacy consultants. More time will be spent by internal and external accounting and legal teams for scheduled audits and for random audits that the member state may execute. Cloud service providers already meet outsourcing guidelines regulations that were published by the EU, for example (EBA, 2019; EIOPA, 2020; Esma, 2020). Such regulations implemented by cloud service providers can save lots of time for organizations looking to comply with existing and future regulations. Giant cloud service providers can most likely quickly adopt and maintain any adjustments to these regulations. It is easier for customers to go through their checklist compared to other on-premises solutions that need to invent the wheel from scratch. Additionally, enterprise software vendors using cloud service provider platforms can leverage the providers' new features and incorporate them into their application solutions.

5. Discussion

Over the last decade, many researchers showed that data privacy regulations slow cloud adoption. Organizations have been more reluctant about migrating to the cloud to ensure they do not violate the regulation, such as keeping the data under the same sovereignty it was collected from and creating isolated networks from the internet to reduce risks. The following studies discuss in more detail the challenges when migrating to the cloud: (Bhayal, 2011; Boillat and Legner, 2013; Gai, 2014; Gumbi and Mnkandla, 2015; Griffith and Stewart 2020; Ivan and Ille, 2021; Meersman and Mulchahey, 2019; Taylor, 2018).

When GDPR became effective, cloud service providers made a significant effort to meet its requirements. They leveraged the opportunity to help their customers comply faster and to increase their income and profit by a broader offering of Platform as a Service (PaaS) supported GDPR features (Spasic *et al.*, 2019). In recent years, there has been a paradoxical trend where organizations are increasingly adopting cloud computing technology to comply with their regulatory requirements and enhance their capabilities. This trend has resulted in a significant increase in the number of organizations embracing cloud computing, even those that were previously hesitant to do so. According to IDC (2022), this trend is expected to continue, with more organizations adopting cloud computing in the coming years. The shift towards cloud computing has been facilitated by government support, as Evidenced by the release of guidelines such as "Guidelines on outsourcing to cloud service providers" by EIOPA (2019).

The paradox effect may even significantly change in the future when hackers and nation-state threat actors find that, in some cases, an on-premises environment would be more vulnerable to attacks because they may not meet the rate of changes in regulatory requirements and hardening which are monitored regularly in cloud mode.

Some defense, governmental, financial, public, or other conservative, strict organizations may decide not to migrate to the cloud and prefer to rely on strict segregation of networks wholly isolated from the internet. However, at some point, they may lose capabilities and support with the tools and technology solutions they operate. Such organizations should consider in-house development, implementing hybrid cloud, gradually migrating some of their environment to the cloud, or working with vendors who offer enhanced regulations features in on-premises mode.

The limitation of this paper is that the regulations are still at a very early stage prior to legislation by member states. Some of the recommendations of cloud providers are under discussion, for example (Microsoft, 2023b). It is possible that within the year, some of the regulations will be softened. Cloud

providers, enterprise software vendors and legal teams are currently still in the review and learning stages.

The intricate interplay between cloud adoption, regulatory compliance, and the overarching cybersecurity landscape adds a nuanced layer to understanding the broader ramifications of the discussed regulations on the EU's overall cyber resilience. Furthermore, the contribution of this paper to the existing literature lies in its exploration of the paradoxical trend observed in recent years, where regulatory compliance drives increased cloud adoption. By delving into the challenges and shifts in organizational behavior, this study sheds light on a dynamic that has not been extensively covered in the current literature, offering valuable insights into the evolving relationship between regulations, cloud adoption, and cybersecurity resilience.

Conclusions

The descriptive literature review, narrative analysis and thematic synthesis uncovered a gap of knowledge and a lack of discussion and research about the new regulations NIS2 and DORA. The main themes derived and common key insights and important trends were explored regarding the potential effects of the regulations on cloud adoption and EU resilience in the coming years.

First, challenges with preparation for the regulations are expected to increase. From a budgetary perspective, it is recommended that organizations allocate sufficient funds towards resilience and cybersecurity tools, as well as engage consultants and legal experts to reassess third-party contracts. This will enable them to invest in more effective cybersecurity and resilience tools, thereby simplifying their implementation process. Moreover, an in-depth exploration of the literature synthesis highlights the need for proactive measures in addressing challenges related to resource constraints, training deficiencies, and supply chain vulnerabilities across various sectors building upon the lessons learned from the GDPR implementation. On the macro side, it may affect the global turnover in investments in the cybersecurity and resilience industry. Failing to comply due to breaches of threat actors will affect national security, especially in ICT, healthcare, and finance markets. The literature synthesis underlines the interconnectedness of national security and compliance, emphasizing the need for comprehensive strategies that address the specific vulnerabilities within each sector. Drawing parallels to the GDPR's impact on global data privacy practices, the literature synthesis establishes the relevance of past regulatory experiences in shaping future strategies.

From a readiness perspective, sectors defined as essential and important which are affected by the regulations face a challenge in complying with it because many of these sectors use old legacy systems and have interconnected systems dependency. Some of these sectors use industrial control

systems (ICS) like Scada, which contains ICS vulnerabilities. In some sectors like healthcare, different organizations use different systems and there is a lack of consistency. The literature synthesis emphasizes the need for sector-specific readiness assessments and tailored strategies to address the unique challenges and complexities within each sector, mirroring the diverse responses observed during the GDPR implementation. Most of these sectors have limited resources, a lack of training for employees, a lack of budget for cybersecurity, and a risk of supply chain vulnerability. Some of these sectors, like transportation, use smart connected IoT devices. Others have third-party risks, large complex systems, and limited resources.

Second, as the scope of the NIS2 directive broadens to include additional sectors, hundreds of thousands of organizations are expected to be affected. To avoid hefty penalties ranging from seven to ten million euros or 1.4%-2% of their global annual turnover, many of these organizations are likely to allocate more funds towards compliance efforts. It is worth noting that the specific penalty amount will be determined by selecting the higher number of the two options for essential and important entities. The literature synthesis provides insights into the potential financial impacts and underscores the necessity for organizations to strategically allocate resources to comply with the evolving regulatory landscape. Referencing the GDPR's influence on global data protection frameworks, the literature synthesis draws parallels, emphasizing the financial motivations and implications associated with regulatory compliance.

Under the DORA regulations, critical ICT third-party service providers can face fines of up to 1% of their average daily worldwide turnover. For medium and large organizations with global turnovers in the billions of dollars, such fines can amount to dozens or even hundreds of millions of dollars. The literature synthesis emphasizes the substantial financial implications under DORA, highlighting the need for critical ICT service providers to reassess their strategies and fortify their compliance efforts. This echoes the experiences of cloud service providers aligning with GDPR requirements, illustrating the financial repercussions associated with regulatory non-compliance. These significant financial penalties are expected to motivate affected organizations deemed essential or important to comply with the new regulations, potentially driving them towards migrating to modern cloud infrastructure in order to expedite their compliance efforts and meet regulatory deadlines.

Third, cloud providers and enterprise software vendors would continue the race to assist their customers. They should evaluate the implications and act accordingly to add more enhanced features to assist organizations in complying with the regulations. They should listen carefully to their customers, conduct an in-depth analysis of the new regulations, and suggest changes to their product

roadmaps. The literature synthesis indicates that ongoing collaboration between organizations and cloud providers is crucial, emphasizing the role of vendors in proactively supporting compliance efforts and adapting to the evolving regulatory landscape. Reflecting on the GDPR's influence on cloud service providers, the literature synthesis establishes a precedent for providers evolving their services to meet regulatory demands.

Fourth, organizations should consider that early warning detection and technologies to support data protection and resilience are essential to comply with the regulations. They should seriously consider migrating to modern cloud providers offering enhanced features to meet the regulations faster. The literature synthesis underscores the significance of early warning systems and cutting-edge technologies, emphasizing the role of modern cloud providers in facilitating swift compliance with evolving regulations. Drawing connections to the GDPR's emphasis on data protection technologies, the literature synthesis highlights the continuous evolution of cybersecurity measures in response to regulatory mandates.

Future work on this topic is recommended to research the readiness of specific member states that are lagging behind in their reaction to the new regulations, the effect of NIS2 and DORA on on-premises environments, and the broader effect of NIS2 and DORA on other continents. Additionally, the literature synthesis suggests avenues for future research, including in-depth investigations into the readiness of specific member states, the implications of NIS2 and DORA on on-premises environments, and the potential global impact of these regulations beyond the EU borders, building upon the lessons learned from the GDPR's impact on global data protection frameworks and strategies.

Disclosure and conflict of interest

The author of this article is a doctoral student researcher at "Alexandru Ioan Cuza" University of Iasi and was the former COO of TrapX Security (a global leader in deception security technology), which Commvault (a global data protection leader) acquired. Today he works at Commvault as Field Security CTO. ThreatWise solution offered by Commvault is an early warning cloud data protection solution based on TrapX deception technology. The author worked in the high-tech industry for 25 years and has more than 10 years of experience in deception technology solutions. The author has tried to remain unbiased in writing this research.

References

Alnajrani, H. M., and Norman, A. A. (2020), The effects of applying privacy by design to preserve privacy and personal data protection in mobile cloud computing: An exploratory study, *Symmetry*, 12(12), 2039.

Amiri-Zarandi, M., Dara, R. A., Duncan, E., and Fraser, E. D. G. (2022), Big Data Privacy in Smart Farming: A Review, *Sustainability*, 14(15), 9120. https://doi.org/10.3390/su14159120

Barbara, C. G., Lynch, P., and Marsnik, S. J. (2001), US multinational employers: Navigating through the "safe harbor" principles to comply with the EU data privacy directive, *American Business Law Journal*, 38(4), 735-783.

Bartlett, T. (2020), *Privacy and Security Management Practices of Emerging Technologies: Internet of Things*, PhD thesis (Order No. 28000028). Available from Publicly Available Content Database (2461614134).

Bhayal, S. (2011), *A study of security in cloud computing*, California State University, Long Beach.

Biasin, E., and Kamenjašević, E. (2022), Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals, *International Cybersecurity Law Review*, 3(1), 163-180.

Boillat, T. and Legner, C. (2013), From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models, *Journal of theoretical and applied electronic commerce research*, 8(3), pp.39-58.

Chazan, G. (2017), SAP raises fears over EU data privacy rules, *Financial* Times, FT.Com.

Express Computer (2018), 83% Indian IT security practitioners believe managing privacy & data protection regulations in cloud is more complicated than on-premises networks, *Express Computer*.

Copeland, L., Jr. (2021), *Developing National Cybersecurity Data and Privacy Protection*, PhD dissertation (Order No. 28963520). Available from Publicly Available Content Database (2634881999).

Corliss, M. (2010), *The use of information: How new technology is changing discussions of privacy*, Master dissertation (Order No. 1475484). Available from Publicly Available Content Database. (305206632).

Cronin, P., Ryan, F., and Coughlan, M. (2008), Undertaking a literature review: a step-by-step approach, *British journal of nursing*, 17(1), 38-43.

Cutler, S. (2018), The face-off between data privacy and discovery: why US courts should respect EU data privacy law when considering the production of protected information, *Boston College Law Review*, 59(4), 1513-1540.

Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 (2022), retrieved from https://www.digital-operational-resilience-act.com/ (Accessed: 26 February 2023).

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 (2022) retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Domingo-Ferrer, J., and Soria-Comas, J. (2015), From t-closeness to differential privacy and vice versa in data anonymization, *Knowledge-Based Systems*, 74, 151-158.

ESMA publishes cloud outsourcing guidelines. (2023), retrieved 30 March 2023, from https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines

Finland: NIS2 Directive strengthens cybersecurity across the EU National implementation launched in January (2023, Jan 11), MENA Report London: SyndiGate Media Inc.

Ford, A., Al-Nemrat, A., Ghorashi, S. A., and Davidson, J. (2021), *The Impact of GDPR Infringement Fines on the Market Value of Firms*, Academic Conferences International Limited. https://doi.org/10.34190/EWS.21.088

Free Word Cloud Generator (2023), retrieved 2 April 2023, from https://www.freewordcloudgenerator.com/generatewordcloud

Gai, K. (2014), A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances, *International Journal of Computer Applications*, 95(3), pp. 40-44.

Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations (2023), retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w (Accessed: 26 February 2023)

General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 (2018) Official Legal Text (2023), retrieved from https://gdpr-info.eu/ (Accessed: 26 February 2023).

Georgiou, D., and Lambrinoudakis, C. (2020), Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR), *Information*, 11(12), 586.

Glova, A. O. (2022), *Architectural Support and Modeling of Emerging Technologies for Datacenter Privacy and Security Applications*, PhD dissertation (Order No. 29325081). Available from Publicly Available Content Database (2729050668).

Google (2023a), *8 megatrends drive cloud adoption—and improve security for all*, Google Cloud Blog (2023), retrieved 25 March 2023, from https://cloud.google.com/blog/products/identity-security/8-megatrends-drive-cloud-adoption-and-improve-security-for-all

Google (2023b), *DORA's implementation period starts now. What we're doing to prepare for the new law*, Google Cloud Blog. (2023), retrieved 25 March 2023, from https://cloud.google.com/blog/products/identity-security/doras-implementation-period-starts-now-what-were-doing-to-prepare-for-the-new-law

Google (2023c), *How Google Cloud is preparing for NIS2 and supporting a stronger European cyber ecosystem*, Google Cloud Blog. (2023), retrieved 25 March 2023, from https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-preparing-for-nis2-and-protecting-europe-from-cyber-threats

Green, B. N., Johnson, C. D., and Adams, A. (2006), Writing narrative literature reviews for peer-reviewed journals: secrets of the trade, *Journal of chiropractic medicine*, 5(3), 101-117.

Griffith, L.D. (2020), Strategies Federal Government I.T. Project Managers Use to Migrate I.T. Systems to the Cloud, Walden University.

Guidelines on outsourcing arrangements - European Banking Authority (2019) retrieved 30 March 2023, from https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

Guidelines on outsourcing to cloud service providers (2023), retrieved 30 March 2023, from https://www.eiopa.europa.eu/publications/guidelines-outsourcing-cloud-service-providers_en

Gumbi, L.N. and Mnkandla, E. (201), Investigating South African Vendors' cloud computing value proposition to small, medium and micro enterprises: a case of the City of Tshwane Metropolitan Municipality, *The African Journal of Information Systems*, 7(4), p.1.

IBM Unveils Z15 With Industry-First Data Privacy Capabilities (2019), Communications Today Information Technology Industry Council: Tech Industry Welcomes Vote on NIS2 Directive, 2021, Oct 29, Targeted News Service.

ITI Offers Recommendations for NIS2 Trilogue Negotiations (2022), Washington, DC.

ITI: Tech Industry Welcomes Vote on NIS2 Directive (2021), Washington, DC.

Ivan, T.R. and Ille, E.E. (2021), *Applying Multi-Criteria Decision-Making to the Technology Investment Decision-Making Process*, Acquisition Research Program.

Jacuch, A. (2021), Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies, *Online Journal Modelling the New Europe*, 37, 102-120. https://doi.org/10.24193/OJMNE.2021.37.06

Jain, P., Gyanchandani, M., and Khare, N. (2016), Big data privacy: a technological perspective and review, *Journal of Big Data*, 3(1), 1-25. https://doi.org/10.1186/s40537-016-0059-y

Johnson, G. A., Shriver, S. K., and Goldberg, S. G. (2023), Privacy and market concentration: intended and unintended consequences of the GDPR, *Management Science*. https://doi.org/10.1287/mnsc.2023.4709

King, W. R., and He, J. (2005), Understanding the role and methods of meta-analysis in IS research, *Communications of the Association for Information Systems*, 16(1), 32.

Ko, S. Y., Jeon, K., and Morales, R. (2011), The HybrEx Model for Confidentiality and Privacy in Cloud Computing, *HotCloud*, 11, 8-8.

Levy, Y., and Ellis, T. J. (2006), A systems approach to conduct an effective literature review in support of information systems research, *Informing Science*, 9.

Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007), l-diversity: Privacy beyond k-anonymity, *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1), 3-es. DOI:10.1145/1217299.1217300

Mahanan, W., Chaovalitwongse, W. A., and Natwichai, J. (2021), Data privacy preservation algorithm with k-anonymity, *World Wide Web*, 24, pp. 1551-1561.

Meersman, M.W. (2019), *Developing a Cloud Computing Risk Assessment Instrument for Small to Medium Sized Enterprises: A Qualitative Case Study Using a Delphi Technique*, Doctoral dissertation, Northcentral University.

Microsoft (2023a), Policy position paper EU cyber resilience act proposal. (n.d.), retrieved March 25, 2023, from https://blogs.microsoft.com//Microsoft-Policy-Paper-Cyber-Resilience-Act-January-2023.pdf

Microsoft (2023b), provided a set of recommendations chrome-extension: //efaidnbmnnnibpcajpcglclefindmkaj/https://blogs.microsoft.com/wp-content/uploads/prod/sites/73/2023/02/Microsoft-Policy-Paper-Cyber-Resilience-Act-January-2023.pdf

Murgia, M., and Coulter, M. (2019), Blockbuster GDPR fines proves boost for cyber protection firms, *Financial Times.*

Nauwelaerts, W. (2004), How EU Data Privacy Affects Due Diligence, *International Financial Law Review*, *23*, 41.

NIS 2 Directive (2023), retrieved from https://www.nis-2-directive.com/ (Accessed: 26 February 2023).

NIS2 is coming… What does it mean? (2022), retrieved 25 March 2023, from https://www.splunk.com/en_us/blog/security/nis2-is-coming-what-does-it-mean.html

Oracle (2023) *What is GRPR?* retrieved 14 April 2023, from https://www.oracle.com/il-en/security/gdpr/

Paré, G., Trudel, M. C., Jaana, M., and Kitsiou, S. (2015), Synthesizing information systems knowledge: A typology of literature reviews, *Information & Management*, 52(2), 183-199.

Perdereaux-Weekes, A. (2021), To Investigate the Impact of Data Privacy Regulation on Disclosure Decisions: Examining Consumers' Willingness to Share or Withhold Personal Identifiable Information in the Wake of GDPR, CCPA, and LGDP, St. Thomas University.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015), Guidelines for conducting systematic mapping studies in software engineering: An update, *Information and software technology*, 64, 1-18.

Phil's Stock World: Google Accused of Intentionally Breaking EU Data-Privacy Laws; YouTube Pays $170M Fine For US Violations (2019). Newstex.

Raghavan, A., Demircioglu, M. A., and Taeihagh, A. (2021), Public health innovation through cloud adoption: a comparative analysis of drivers and barriers in Japan, South Korea, and Singapore, *International Journal of Environmental Research and Public Health*, 18(1), 334.

Rajamäki, J. (2021), Resilience Management Concept for Railways and Metro Cyber-Physical Systems, Academic Conferences International Limited. https://doi.org/10.34190/EWS.21.074

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Ross, W. (2018), EU data privacy laws are likely to create barriers to trade, *Financial Times*.

Schmitz-Berndt, S., and Chiara, P. G. (2022), One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive, *International Cybersecurity Law Review*, 3(2), 289-311.

Singh, N., and Singh, A. K. (2018), Data Privacy Protection Mechanisms in Cloud, *Data Science and Engineering*, 3(1), 24-39. https://doi.org/10.1007/s41019-017-0046-0

Spasic, B., Boucart, N., and Thiran, P. (2019), Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure, *Computers*, 8(2), 34. https://doi.org/10.3390/computers8020034

Strengthening EU-Wide Cybersecurity and Resilience - Provisional Agreement by the Council and the European Parliament. (2022, May 14), Targeted News Service

Taylor, C.M., Sr. (2018), *Identifying and Overcoming the Barriers to Cloud Adoption within the Government Space*, The George Washington University.

Taylor, P. (2011), Privacy concerns slow cloud adoption, *Financial Times.*

The Threat Report: February 2023, Trellix (2023), retrieved 2 April 2023, from https://www.trellix.com/en-us/advanced-research-center/threat-reports/feb-2023.html

Tzanou, M. (2020), The future of EU data privacy law: towards a more egalitarian data privacy, *Journal of International and Comparative Law*, 7(2), pp. 449-469.

Venkataramakrishnan, S. (2021), GDPR fines jump as EU regulators raise pressure on business, *Financial Times*.