Master Thesis

Navigating Europe's Digital Services Act: Challenges for Online Platforms

Q.A.H. Hulshof (Quint)

April 30, 2024

Faculty of Behavioural, Management and Social Sciences

Master Business Administration

Track Digital Business & Analytics

Supervisors

Dr. A. Abhishta, Faculty of BMS and IEBIS

Dr. Ir. A.A.M. Spil, Faculty of BMS and IEBIS

UNIVERSITY OF TWENTE.

Ms. Rebecca Hulleman, Senior Consultant

IT Assurance & Advisory

KPMG

Acknowledgements

I extend my deepest thanks to my supervisor, Rebecca Hulleman, for her invaluable guidance and steadfast support throughout my thesis journey. Our collaboration was not only enjoyable but also fruitful, resulting in a thesis I am proud of. My gratitude also goes to KPMG for offering me the chance to conduct my research in partnership with their respected organization. This opened doors to an extensive amount of knowledge and expertise, greatly enriching my research experience.

Furthermore, I am immensely grateful to my academic supervisors from the University of Twente, Dr. A. Abhishta and Dr. Ir. A.A.M. Spil, for their expert mentorship and guidance in the intricate world of academic research. Their profound knowledge and advice have been essential to my academic growth and development, for which I am truly thankful.

Lastly, I must acknowledge the valuable input of all the experts who dedicated their time and shared their knowledge and expertise with me. Their insights have been an essential component of my study, significantly improving its quality and expanding my understanding of the subject.

Management Summary

The Digital Services Act (DSA) introduces a new era of regulatory requirements for online platforms, aiming to enhance digital safety by protecting user rights and ensuring fair business practices. The act mandates robust measures to address risks associated with illegal content, misinformation, and harmful online behaviours. These include advanced content moderation, transparency in algorithms, and user empowerment over content visibility. Furthermore, very large platforms are subjected to additional scrutiny through mandatory risk assessments and independent audits.

This broad array of requirements presents significant challenges for online platforms, and since the DSA was recently introduced, there is a notable lack of comprehensive literature on these challenges. Available sources often only provide speculative analyses of the potential impact of the legislation but offer little concrete insight into the practical challenges that platforms face. Therefore, this study will try to fill this gap and provide detailed insights into the legal and operational challenges companies face in complying with the DSA. It does so through the following research question: *'How can expert opinions be leveraged to deepen our understanding of the legal and operational challenges online platforms face in complying with the Digital Services Act (DSA), and how can these challenges be effectively addressed?'*

To provide online platforms and other stakeholders with insights and practical solutions for navigating the requirements of the DSA, this study is structured into two main parts. In the first part, due to the scarcity of literature, in addition to the DSA, the GDPR is also examined to investigate whether parallels can be drawn. First, the requirements of both legislations are analysed. Then, based on these requirements, two systematic literature reviews (SLRs) on the GDPR and the DSA are conducted to identify the legal and operational challenges that online platforms experience in becoming compliant with these regulations. The overview that emerges from this will form the basis for the empirical part of this research.

The second part of this study delves deeper into the specific challenges of the DSA through interviews with experts in digital law, IT audit, and representatives from online platforms. The resulting insights provide greater detail into the operational challenges experienced by online platforms and other stakeholders, as well as how they are addressing these challenges. Ultimately, findings from the interviews and literature are used to develop a risk mitigation framework that provides actionable insights and recommendations for navigating DSA compliance.

Key findings from this research illustrate the significant challenges faced by online platforms under the DSA. These challenges mainly arise from vague legal terms and ambiguities, compounded by a lack of clear guidelines, which create significant barriers to compliance. Additionally, the decentralized nature of platform operations and rapid development cycles make it difficult to gain a holistic understanding of the necessary operational changes. This complexity is especially pronounced when platforms attempt to expand or upgrade their system capabilities to effectively manage the volume, variety, and complexity of user-generated content. Furthermore, the research highlights the urgent need for centralized leadership and the creation of cross-functional teams. These measures are critical to ensure that DSA compliance is harmonized across departments and that strategic approaches are effectively aligned, improving overall regulatory compliance.

Based on these insights, several expert-informed strategies have emerged to effectively navigate the legal and operational complexities of the DSA. The recommendations advocate a proactive and strategic approach to compliance. This includes developing robust internal compliance frameworks that provide clear, actionable guidance to demystify DSA requirements and ensure a uniform approach across regulatory landscapes. It is also essential to improve collaboration between teams within

platforms and with external stakeholders, including regulators and auditors, to advocate for more comprehensive guidelines and standardized audit protocols. Platforms must invest in technology and in-house expertise to build advanced content moderation systems and address the complexity of user-generated content. In addition, they should initiate early preparation for audits and develop standardized audit processes in collaboration with stakeholders to ensure consistency and reliability in compliance assurance assessments.

In addition, the European Commission (EC) and national regulatory authorities are urged to issue detailed guidelines and frameworks to reduce ambiguity and promote consistent application across platforms. These agencies should also increase their engagement with stakeholders to refine the implementation process and address structural enforcement capacity gaps by recruiting staff with the right competencies.

Auditors are recommended to collaborate closely with online platforms to develop clear and standardized audit protocols. Additionally, there is a significant business opportunity for advisory services to offer specialized knowledge in digital law, risk management, and compliance strategies. Conducting a thorough market analysis to confirm these needs will be crucial for auditors and advisory firms to establish a leading position in the market for digital compliance.

This thesis not only contributes to academic discussions on data protection and digital services, but also provides a practical guide for organizations navigating the complex landscape of digital compliance. Using expert opinions and empirical data, it provides a first comprehensive overview of the challenges and strategies related to DSA compliance, aimed at facilitating more effective and efficient regulatory practices.

Table of Contents

1 Introduction

In the digital age, the internet has evolved into an intricate web of information, communication, and commerce, shaping the way we live, work, and interact [1]. As a result, our personal data and online experiences have become invaluable commodities, drawing the attention of regulators worldwide [2]. In Europe, two legislations stand at the forefront of this regulatory landscape, namely the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). Together, they present a complex set of regulations that challenges online platforms operating within the European Union.

1.1 Background

The GDPR, introduced in 2018, was a turning point in data protection, setting a global standard for safeguarding individuals' privacy rights in the digital domain. It demanded that organizations treat personal data with the utmost care, requiring transparency, accountability, and stringent compliance [3]. On the other hand, the DSA, proposed in late 2020, aims to address a broader spectrum of digital issues, focusing on online content moderation, oversight structure, and platform transparency [4]. While the GDPR primarily deals with data protection, the DSA encompasses a wider range of digital services and content, making the regulatory landscape increasingly intricate.

With the introduction of the DSA, additional requirements are once again imposed on these online enterprises. In preparation for the DSA, the European Commission conducted stress tests on several platforms, including, Facebook, Instagram, TikTok and X. The findings indicated that, in every case, additional measures were necessary for these platforms to meet the DSA's requirements [5]. For these companies, compliance is a must, since a violation of the DSA could result in penalties of up to 6% of their worldwide revenue, and those infringing repeatedly may face a total ban on their operations within Europe.

1.2 Problem Statement & Research Goal

Navigating these regulations poses significant challenges for online platforms in Europe, as they grapple with compliance obligations that sometimes seem to overlap or even conflict [6]. By exploring the key legal and operational challenges faced by online platforms we seek to shed light on the complexities of this regulatory environment and provide actionable insights to help organizations thrive in this evolving digital landscape.

Given the recent introduction of the DSA, there is a scarcity of comprehensive literature on this topic. Existing sources often include opinions and speculative analysis on the impact of regulations. Therefore, despite the obvious differences between the two pieces of legislation, this thesis will explore the legal and operational challenges that organizations have encountered in their efforts to comply with the GDPR. The purpose of this is to gather insights that can be important in identifying and addressing the challenges posed by the DSA. With this comparative analysis, based on challenges and lessons learned from GDPR compliance, we ultimately aim to equip online platforms, auditors and regulators with challenges and possible solutions they can expect as they navigate the complexities of the DSA.

In this thesis, we will delve into literature on both regulations and, in this way, carry out an in-depth analysis, as well as explore practical implications through interviews with experts in the field of digital law, IT audit, and representatives from platforms dealing with the DSA. We do this to provide further explanation into the challenges they experience with the aim of equipping online platforms with the knowledge and strategies needed to effectively navigate this complex regulatory environment. In doing so, we not only contribute to the research conversation on data protection and digital services, but we

also try to provide practical solutions to the challenges that online platforms face in the digital age. In this thesis we will answer the following central research question:

'How can expert opinions be leveraged to deepen our understanding of the legal and operational challenges online platforms face in complying with the Digital Services Act (DSA), and how can these challenges be effectively addressed?'

To answer this main research question, the following sub questions will be addressed:

1. What are the requirements that online platforms must meet according to the GDPR?
2. What are the requirements that online platforms must meet according to the DSA?
3. What legal and operational challenges do online platforms face when implementing GDPR, as discussed in literature?
4. What legal and operational challenges do online platforms face when implementing DSA, as discussed in literature?
5. How do experts validate and enhance the findings regarding the challenges online platforms face with DSA compliance, as discussed in literature?

1.3 KPMG

This thesis will be written with the support and guidance professionals in the KPMG network. KPMG, or Klynveld Peat Marwick Goerdeler, is one of the world's leading professional services firms, specializing in audit, tax, and advisory services. Founded in the Netherlands in 1917, KPMG has grown into a global network of member firms with a presence in over 150 countries and territories, making it one of the "Big Four" accounting firms alongside Deloitte, PricewaterhouseCoopers (PwC), and Ernst & Young (EY) [7], [8].

The company's primary operations are divided into two core segments: Assurance and Advisory, with dedicated support from their Business Services function. Approximately 60% of KPMG N.V.'s revenue is generated from their assurance business, encompassing both financial and non-financial assurance services. This includes the auditing of financial statements, accounts, IT, and regulatory disclosures across various sectors, including Corporate Clients, Financial Services, Public Sector & Healthcare, International Business, and Private Enterprises [7].

This research has been carried out within the KPMG IT Assurance department, which provides companies in the Netherlands with IT auditing, assurance, and advice. In the context of this study, KPMG has played an important role in providing valuable guidance and advice to online platforms within the constantly evolving landscape of data protection and digital services.

1.4 Methodology

In this paragraph, we briefly outline the approach we have adopted for our research. A more detailed explanation of the various research methods is presented at the outset of each chapter. This ensures a thorough understanding of the methodologies employed throughout this study.

Given the novelty of the DSA, we advocate for an exploratory and qualitative research methodology. This allows us to delve deeply into the complexities and nuances of the DSA, providing a comprehensive understanding of its implications and potential impacts.

In the following chapter, we carry out a detailed analysis of the legal texts of the GDPR and DSA, published articles from the European Commission, and selected academic studies. With this, we aim to understand the background and foundational aspects of these regulations. The goal is to synthesize

this information and present a clear overview of the obligations and requirements online platforms must meet in accordance with the GDPR and DSA.

In Chapter 3, with a thorough understanding of the requirements for both regulations established, we perform two systematic literature reviews (SLRs) to explore existing literature and articles on the challenges companies face in complying with both the GDPR and DSA. To perform these reviews we use parts of the systematic literature review technique by Kitchenham (2004), [9].

In addition to the gathering of secondary data, in Chapter 4, we conduct semi-structured interviews with experts in the field of digital law, IT audit, and representatives from platforms dealing with the DSA. Participants are chosen using purposeful and snowball sampling approaches, and data collection will end when saturation is reached. For conducting the semi-structured interviews, the methodological strategy of Adeoye-Olatunde and Olenik (2021), [10], is used. An overview of the research methods used to answer each sub question, along with the expected results, can be found table 1.

Table 1 Methodology and result per sub question.

Nr	Sub question	Methodology	Result
1.	What are the requirements that online platforms must meet according to the GDPR?	Literature and legal text	Overview of requirement for online platforms
2.	What are the requirements that online platforms must meet according to the DSA?	Literature and legal text	Overview of requirement for online platforms
3.	What legal and operational challenges do online platforms face when implementing GDPR, as discussed in literature?	SLR	Overview of challenges for online platforms
4.	What legal and operational challenges do online platforms face when implementing DSA, as discussed in literature?	SLR	Overview of challenges for online platforms
5.	How do experts validate and enhance the findings regarding the challenges online platforms face with DSA compliance, as discussed in literature?	Semi-structured interviews	Validation and exploration of challenges and recommendations

1.5 Approach

In this paragraph, we describe our approach and the decisions we made in this report. Initially, our research focused solely on the DSA. However, it quickly became evident from the literature that, due to its recent introduction, there was predominantly speculation with scarce discussion of the actual challenges faced by online platforms. Consequently, we shifted our attention to the GDPR to derive insights from its compliance challenges. This SLR not only highlighted specific challenges related to GDPR but also identified broader compliance issues applicable to multiple new regulations. These challenges, together with those mentioned in the literature for the DSA, which were quite general and had to be generalized considerably, formed the basis for the interviews with experts.

The initial goal of our research was to identify and provide more detail on these challenges. Eventually, with the information obtained from the interviews, we made the decision to develop a framework that addressed these challenges and the risks they posed, providing a first step for companies to tackle these risks. In the final phase of the research, based on the knowledge gained during the study, we adjusted the main research question to its current form. Initially, it primarily addressed the legal and

operational challenges that companies faced in complying with the GDPR and DSA, later evolving to incorporate the expert perspectives we had gathered.

1.6 Structure

In Chapter 2 of this study, the requirements that companies must meet under the GDPR and DSA are analysed and summarized in two tables. Chapter 3 explores these requirements through two systematic literature reviews (SLRs) to identify challenges companies face in achieving compliance with these regulations. At the end of Chapter 3, these challenges will be analysed. These challenges, identified in the literature, then form the basis in Chapter 4, Results, for conducting and holding interviews with experts. Later in this chapter, a risk mitigation framework is developed based on the themes that emerged during the interviews, with the aim of providing concrete guidelines to online platforms on how to address these challenges. Chapter 5 includes a discussion of the results and explores potential next steps for stakeholders, including online platforms, the EC and regulatory bodies, and auditors. Finally, Chapter 6 will conclude this study and provide answers to the main research question as well as offer recommendations.

2 Background and Related Studies

To grasp the challenges that online platforms face while dealing with these regulations, it is first essential to comprehend the requirements they are obligated to adhere to. Therefore, in this chapter, we analyse the legal texts of both the GDPR and the DSA along with published articles from the European Commission and selected academic studies. With this our goal is to provide a comprehensive overview of both pieces of legislation. If you are already acquainted with these laws, you may choose to skip this chapter. As this topic is not the primary focus of our study, only a brief introduction and the results will be presented here. For more detailed background information on the history and evolution of the GDPR, as well as a detailed analysis of the different chapters in the law, please refer to Appendix A.

This chapter starts with an introduction to the GDPR, after which the GDPR requirements for online platforms are summarized in a table. Subsequently, we adopt a similar approach to the DSA, summarizing its requirements in a table as well, equipping us with the necessary knowledge to explore these challenges in the literature. The last paragraph briefly explains what is meant by legal and operational challenges in this study.

2.1 The General Data Protection Regulation (GDPR)

As technology rapidly advanced in the early 21st century, new challenges emerged in the realm of data protection [11]. The increasing prevalence of the internet, e-commerce, and social media raised concerns about the adequacy of existing regulations to address the complexities of digital data processing. An update of regulations was needed, the European Data Protection Supervisor recognised this and published an opinion on the European Commission in June 2011 [12]. This kickstarted the reform of the EU's 1995 Data Protection Directive to strengthen online privacy rights and boost Europe's digital economy. After several years and multiple recommendations and updates, the European Parliament, Council, and Commission reached an agreement on the reformation of the GDPR, and 2 years later, on May 25, 2018, it came into effect [13].

As technology rapidly developed in the early 21st century, new data protection challenges emerged worldwide[11]. The increasing prevalence of the Internet, e-commerce and social media raised concerns about the adequacy of existing regulations to address the complexities of digital data processing. The European Data Protection Supervisor recognized the need for an update and published an opinion on the European Commission in June 2011 [12]. This initiated the reform of the 1995 EU Data Protection Directive to strengthen online privacy rights and boost Europe's digital economy. After several years and multiple recommendations and updates, the European Parliament, Council, and Commission reached an agreement on the reformation of the GDPR, and 2 years later, on May 25, 2018, it came into effect [13].

The GDPR represents a significant evolution in data protection, designed to give individuals more control over their personal data. It applies to all organizations operating within the EU and to international companies that process the personal data of EU residents. The regulation emphasizes transparency, security and accountability, requiring organizations to take comprehensive measures to protect data [12]. Online platforms, ranging from social media giants to e-commerce websites, often find themselves at the epicentre of GDPR compliance due to their nature as personal data-intensive companies. The regulation not only requires these platforms to obtain clear and explicit consent before collecting and processing user data but also mandates transparent communication regarding the purpose and duration of data processing [14]. The global impact of the GDPR is profound and sets a new standard for privacy rights in the digital age.

2.2 Summary of GDPR Requirements

To provide a comprehensive picture of the implications for online platforms when handling personal data, we have summarized the GDPR requirements in Table 2, which also answers sub question one of this study. This table takes a closer look at four crucial aspects of the GDPR: legal basis and transparency, data security, liability and governance, and privacy rights. The data used to compile this table comes directly from the GDPR legal text and is supplemented with information from the European Commission [15]. This table provides insight into the requirements that companies must meet, and therefore gives us sufficient tools to search the literature for challenges that companies experience with GDPR compliance. For more details on the different articles in the GDPR and the compilation of this table, please refer to Appendix A.

Table 2 Summarized GDPR requirements.

Requirement	**Brief Explanation**
	Lawful basis and Transparency
Information Audit	Organizations, especially those with 250 or more employees, must maintain an updated list of processing activities, including purposes, data types, access details, third-party involvement, data protection measures, and deletion plans.
Legal Justification	Data processing must align with one of the six conditions in Article 6 of the GDPR. Additional provisions for children and special categories of personal data (Articles 7-11) should be considered. Legal bases must be documented, especially if relying on "consent" or "legitimate interests."
Privacy Policy	Clear and concise information about data processing and legal justification must be provided in the privacy policy. The information should be easily accessible and understandable, particularly for children.
	Data Security
Data Protection by Design and Default	Organizations must integrate data protection principles into product development and data processing, implementing appropriate technical and organizational measures. Encryption, pseudonymization, and adherence to Article 5 principles are essential.
Encryption, Pseudonymization	Utilize encryption, pseudonymization, or anonymization of personal data wherever possible, especially in widely used productivity tools that offer end-to-end encryption.
Internal Security Policy	Establish an internal security policy covering email security, passwords, two-factor authentication, device encryption, VPN usage, and provide training to ensure team members are knowledgeable about data security.
Data Protection Impact Assessment	Perform a data protection impact assessment whenever processing activities pose a high risk to individuals' rights and freedoms. Have a process in place to analyse and minimize risks.
Data Breach Notification	In the event of a data breach, notify the supervisory authority within 72 hours and communicate breaches to data subjects promptly, unless the breach is unlikely to put them at risk. Authorities in non-EU countries may include the Office of the Data Protection Commissioner in Ireland.
	Accountability and Governance
GDPR Compliance Accountability	Designate a responsible person within your organization to ensure GDPR compliance. This individual should evaluate data protection policies and oversee their implementation.
Data Processing Agreement	Sign a data processing agreement with third parties handling personal data on your behalf. These agreements outline rights and obligations for GDPR

	compliance and should be reviewed for reliability and data protection guarantees.
Appointment of Representative	If your organization is outside the EU and processes data related to individuals in a specific member state, appoint a representative within that country to communicate with data protection authorities.
Data Protection Officer (DPO)	Appoint a Data Protection Officer if required by circumstances or as a proactive measure. The DPO monitors GDPR compliance, assesses data protection risks, advises on impact assessments, and collaborates with regulators.
Privacy Rights	
Right to Information Access	Data subjects have the right to request and receive information about the personal data you have, its usage, storage duration, and the reason for retention. Comply with such requests within a month, and initial copies should be provided for free.
Right to Correct or Update Information	Data subjects can easily correct or update inaccurate or incomplete personal information. Implement a data quality process and facilitate customer access and updates within a month, verifying their identity.
Right to Data Deletion	Data subjects can request the deletion of their personal data, which should be honoured within about a month, except for specific grounds for denial. Identity verification of the requester is necessary.
Right to Stop Data Processing	Data subjects can request to restrict or stop processing their data, honoured within about a month. While processing is restricted, data storage is permitted, and the data subject must be notified before resuming processing.
Right to Data Portability	Data subjects can receive a copy of their personal data in a transferable format. Ensure the ability to send data in a commonly readable format upon request.
Right to Object to Data Processing	Data subjects can object to data processing, particularly for direct marketing purposes, leading to an immediate cessation of processing unless compelling legitimate grounds exist.
Protection of Rights in Automated Decision-Making	Establish procedures for organizations using automated processes for decisions with legal or significant effects. Provide mechanisms for human intervention, allowing individuals to weigh in on decisions and challenge them.

2.3 The Digital Services Act (DSA)

Having mapped out the requirements for the GDPR, we can now proceed to do the same for the DSA. Following this, we will explore the literature to identify challenges associated with these requirements. This section will first provide some background information on the DSA, followed by a detailed elaboration of its requirements. Because the DSA is the main subject of this study, the requirements of this legislation will be discussed in more detail than the requirement of the GDPR.

On 15 December 2020, the European Commission introduced its DSA proposal together with DMA. The Commission considers this to be an important step in the direction of ensuring a safer, fairer digital environment for all. This move came after EU co-legislators reached a consensus in April 2022, leading to the DSA being officially implemented on November 16, 2022 [16], [17].

The DSA builds upon the foundational principles of the e-Commerce Directive, aiming to overhaul the existing framework. The new legislation seeks to establish a modern, robust governance structure across Europe, equipped to address emerging digital challenges [18]. The range of the DSA covers all digital services that connect consumers to various goods, products, or downloadable content. It comes

with a large range of new rules for online platforms that seek to limit risks as well as harm on the internet while introducing strong safeguards for user rights. Furthermore, it subjects digital platforms to an unprecedented framework of transparency and accountability. As uniform regulations for companies operating inside the EU, these rules are intended to provide legal clarity for businesses and give users new rights across the internal market. The DSA is globally unique in its regulatory approach to online platforms and serves as a pioneering model for international digital regulation [16].

In April 2023, the European Commission designated the first 17 very large online platforms (VLOPs). Designated platforms include Meta platforms such as Instagram and Facebook, Alphabet platforms such as Google Maps and Youtube, and other platforms such as Tiktok, Zalando and AliExpress. In addition, they pointed out 2 very large online search engines (VLOSEs), namely Bing and Google Search [16]. At the end of 2023, as a result of an investigation, the Commission added 3 more platforms to the list, namely, Pornhub, Stripchat and XVideos [19].

Next to these VLOPs, all online platforms, hosting services, and intermediary services operating inside the EU are required to adhere to the general obligations of the Digital Services Act (DSA) by February 17, 2024. Micro and small enterprises, which employ less than 50 persons and/or have an annual turnover of less than 10 million euro form an exception [20]. They will be subject to responsibilities that are aligned with their capacity and scale, while still maintaining a level of accountability. An overview of the types of companies that must comply to the DSA, and examples of such companies, can be found in Table 3.

Table 3 Overview of online service providers covered by the DSA [18].

Service providers	Types of companies	Examples
Intermediary services	Internet access providers, content distribution networks, web-based messaging services and local area network providers.	Whatsapp, Skype, Telegram, T-Mobile
Hosting services	Providers of information storage solutions, webhosting, and cloud services.	OVH, AWS, Worldstream, Cloudfair
Online platforms	Social networks, online marketplaces, app stores, online travel and accommodation websites and content sharing websites.	Uber, Airnbnb, Spotify, Etsy, Zoom
VLOPs	Online platforms with more than 45 million monthly users.	Instagram, Tiktok, Zalando, Google Maps.

The Digital Services Act (DSA) introduces new responsibilities for service providers, tailored to their market role, size, and impact. Detailed in Table 4, these obligations are aligned with four main categories of service providers, as previously outlined. The DSA's primary objectives include reducing illegal or potentially harmful online content, defining liability for third-party content on online intermediaries, safeguarding users' Fundamental Rights (FR) online, and addressing informational imbalances between online intermediaries and their users.

The responsibilities of online intermediaries vary depending on their size and the services they offer. The structure of the DSA creates a layered regime of obligations. The lightest regime applies to intermediary services. Additional obligations apply to hosting services. Further responsibilities also apply to online platforms, and most obligations apply to VLOPs and VLOSEs.

Below we will explain the requirements per type of company in order of the articles in the DSA, after which they will be summarized in Table 4.

Liability Waivers

The DSA incorporates the liability exemptions for intermediary services from the Electronic Commerce Directive [21]. These liability exemptions ensure that online intermediary services cannot be held liable if they have not had any substantive involvement in the digital content originating from users that they transmit or host and if they delete this information immediately upon becoming aware that this is illegal (e.g. racist statements). For example, Instagram is not liable for a discriminatory statement on its platform as long as the company has no knowledge of it, and promptly removes the statement if it becomes aware of it.

These liability waivers implied that intermediary services limited their own initiative in searching for unlawful content because they could lose their liability waivers if they became aware of unlawful content. A new provision has now been added to the DSA, which emphasizes that intermediary services will not lose their liability exemption if they voluntarily conduct investigations or take other measures aimed at removing illegal content (Article 7).

Content Moderation

Intermediary services are required to provide information about their content moderation procedures in their general terms and conditions. This information must be publicly available as well as easily accessible.

In addition, annual reporting and publication must be conducted on the content moderation carried out over the past year. Intermediary services must in every instance report on the number of complaints about illegal content, content moderation on their own initiative and information about the use of automated means for content moderation, as described in article 15.

Hosting parties and online platforms must establish additional procedures regarding content moderation. Illegal content must be able to be reported. The reporter must receive confirmation of receipt, be informed of the decision taken and be informed of the options for appeal. In addition, according to article 16 and 17, any content moderation must be explained to the submitter of the content that has been moderated, unless it concerns large-scale misleading commercial content.

Articles 19 to 21 describe that online platforms are additionally obliged to establish free complaint procedures for anyone whose content has been moderated. These platforms must also participate in a system of easily accessible extrajudicial dispute resolution. And if it turns out that the content should not have been moderated, it should also be possible to put it back. Customers who frequently post illegal content may, after warning, be suspended.

Trusted Flaggers

The nationally designated digital services coordinator can appoint so-called reliable flaggers. As specified in Article 22, these are independent parties that have specific expertise in detecting and reporting illegal content. Reports of illegal content originating from these trusted flaggers should be processed and handled by online platforms as a priority.

Advertising Guidelines

Online platforms must make sure that users can easily identify which content on the platform is about advertising and who from whom this content is. According to Article 26, Information should also be provided on what factors are used to determine who sees which advertising. Article 28 adds to this that it is forbidden to advertise to minors or based on certain kinds of personal information, e.g. political preference.

Recommender System Transparency

Online platforms must provide information in their terms and conditions about the key parameters in their recommendation systems and their relative importance compared to each other, as well as any options for the recipients of the service to modify or influence these key parameters (Article 27).

Traceability of Third-party Suppliers (KYBC)

According to Article 30 of the DSA, online platforms are obliged to check and verify the identity of traders who offer services or products to consumers through their platform. If the trader provides incorrect or incomplete information, the online platform shall suspend the trader's use of the platform. If an online platform discovers that a trader offers illegal products or services through the online platform, the online platform is obliged to inform the consumers who purchased these products or services (Article 32).

Additional Requirements for VLOPs and VLOSEs

In addition to all the above items, VLOPs and VLOSEs must meet an additional set of requirements. These parties are obliged, among other things, to periodically audit the systemic risks arising from the design, operation, and use of their services. These include: the distribution of illegal content through their services; the effects on the FR of users such as the right to freedom of expression, the right to private life but also the right to non-discrimination and the rights of minors; the effects on democratic processes (like elections) and the effects on public health and gender-based violence (Article 34).

Article 35 points out that VLOPs and VLOSEs must then take reasonable and effective risk mitigation measures in this context, for example adjusting online interfaces or algorithmic systems.

Digital Services Coordinators and Fines

Each member state of the EU is required to appoint a national Digital Services Coordinator (DSC). These DSCs have the power to conduct investigations, demand accountability and issue fines.

Non-compliance with the requirements specified in the Digital Services Act (DSA) may lead to penalties, such as a fine amounting to a maximum of 6% of the annual global revenue of the relevant service provider, or a prohibition on conducting business within the EU market if there are multiple severe breaches (Article 51 and 52).

2.4 Summary of DSA Requirements

To provide a comprehensive view of the implications for online platforms in implementing the DSA, we have summarized the DSA requirements in Table 4. This table shows a clear overview of the DSA's layered regime and requirements for intermediary services, hosting services, online platforms and VLOPs. All the requirements in the text above and in the table are derived from the legal text of the DSA itself. These requirements have been compiled into a table by [4]. This table has been checked for accuracy and compared with the legal text as we have interpreted it. The table was then adopted with a few minor changes, as shown below in Table 4. This table contains all requirements that companies subject to the DSA must meet and therefore answers sub-question 2.

Table 4 New obligations for online service providers in the DSA, adopted from [4].

		Intermediary services	Hosting services	Online platforms	VLOPs
Transparency measures for online platforms	Transparency reporting	√	√	√	√
	Requirements on terms of services due account of fundamental rights	√	√	√	√
	Notice-and-action and obligation to provide information to users		√	√	√

	User-facing transparency of online advertising			√	√
	Transparency of recommender systems and user choice for access of information				√
Oversight structure to address the complexity of the online space	Cooperation with national authorities following orders	√	√	√	√
	Points of contact and, where necessary, legal representative	√	√	√	√
	Complainant and redress mechanism and out of court dispute settlement			√	√
	External risk auditing and public accountability				√
	Crisis response cooperation				√
Measures to counter illegal goods, services, or online content	Trusted flaggers			√	√
	Measure against abusive notices and counter notices			√	√
	Vetting credentials of third-party suppliers (KYBC)			√	√
	Reporting of criminal offences			√	√
	Risk management obligations and compliance officer			√	√
	Codes of conduct				√
Data access for authorities and researchers	Data sharing with authorities and researchers				√

2.5 Definitions of Legal and Operational Challenges

In this paper, legal challenges within organizations are primarily defined as issues related to compliance with laws and regulations. This aspect is essential for ensuring that an organization operates legally and avoids legal disputes that could harm its reputation and financial health. Compliance is key to maintaining the organization's integrity and adapting to the often-changing legal environment.

Operational challenges, in contrast, relate to everyday business management and include, for example, resource allocation, technology, quality control, employee management, and data management, all focused on maintaining efficiency and productivity.

The key difference lies in their focus: legal challenges deal with external compliance and liability protection, requiring legal expertise, while operational challenges involve optimizing internal processes for effective business operations.

3 Theoretical Findings

In this segment of the research, we conduct two systematic literature reviews (SLRs) to explore the challenges companies face in achieving compliance with both the GDPR and the DSA. As mentioned earlier in this thesis, a preliminary review of the literature indicated that there is limited research on the DSA and the challenges companies face in complying with it. Consequently, to better understand the implications of such significant digital legislation, we first examine the GDPR. This approach allows us to explore the legal and operational challenges that companies have encountered when adapting to previous major regulatory changes in the digital landscape. This analysis will provide a foundation for understanding the potential complexities and issues related to the DSA's implementation.

This chapter starts with a description of the development of both SLRs, after which the results of the SLR for the GDPR are briefly discussed. To keep the focus on the core topic, namely the DSA, only the relevant legal and operational challenges are discussed that could also apply to DSA. The GDPR legislation specific challenges are discussed in detail in Appendix B. After the challenges regarding the GDPR, which can provide insight for the DSA, have been discussed, an SLR is also carried out for the DSA. The aim of both these SLRs is to give us an overview of the available literature and to give us a solid basis for the practical part of this research, namely conducting interviews with experts in the field of digital law, IT audit, and representatives from platforms dealing with the DSA.

3.1 Developing the Structured Literature Review

The aim of these SLRs is to represent available literature as correctly and comprehensively as possible. This calls for a process that guarantees the collection of data in an unbiased manner, producing an outcome that accurately reflects the most recent research on a particular subject. To achieve this, we use parts of the Systematic Literature Review technique by Kitchenham (2004), [9]. According to Kitchenham's framework, an SLR can be seen as a way of identifying, evaluating, and interpreting all relevant and available studies on a particular research question, topic area or phenomenon. This method has been chosen for its objective and reproducible way of providing practical evidence and theoretical implications.

3.1.1 Preliminary Search

The goal of the preliminary search was to get acquainted with the subjects and gain knowledge to construct the search string. Additionally, this stage provided related literature that was valuable for writing the background chapter and parts of the introduction. For this search, multiple academic resources were utilized, like Scopus and Web of Science.

3.1.2 Search String

With these SLRs, our aim is to explore existing literature and elaborate on legal and operational challenges that online platforms experience while trying to comply with GDPR and DSA obligations. Based on this and the main research question the following search strings were created.

- ("GDPR" OR "General Data Protection Act") AND ("Challenge*" OR "Difficulties" OR "Complication*") AND ("Business*" OR "Companies" OR "Organization*" OR "Enterprise*" OR "Firm*" OR "Institution*" OR "Entities" OR "Government*")
- For *DSA*: ("Digital Services Act") AND ("Challenge*" OR "Difficulties" OR "Complication*")

The search for GDPR was conducted on November 13, 2023, and the search for DSA was conducted on December 19, 2023. In these search strings an asterisk (*) is used for including articles that use plural denomination. Additionally, an examination of the search strings was conducted to determine if using capital letters or American/English variations would yield different results. However, no noticeable variations in results were observed under these conditions.

When determining the search string for challenges surrounding the GDPR, the initial search was for '("Online platforms" OR "Digital Platforms" OR "Internet platforms" OR "Virtual platforms" OR "Digital Services")' but as this search only returned 11 results it was decided to replace this with broader terms that can be seen above, this ultimately resulted in 491 documents in Scopus and 286 documents in Web of Science. A visual overview of the articles found for the GDPR can be found in Figure 1.

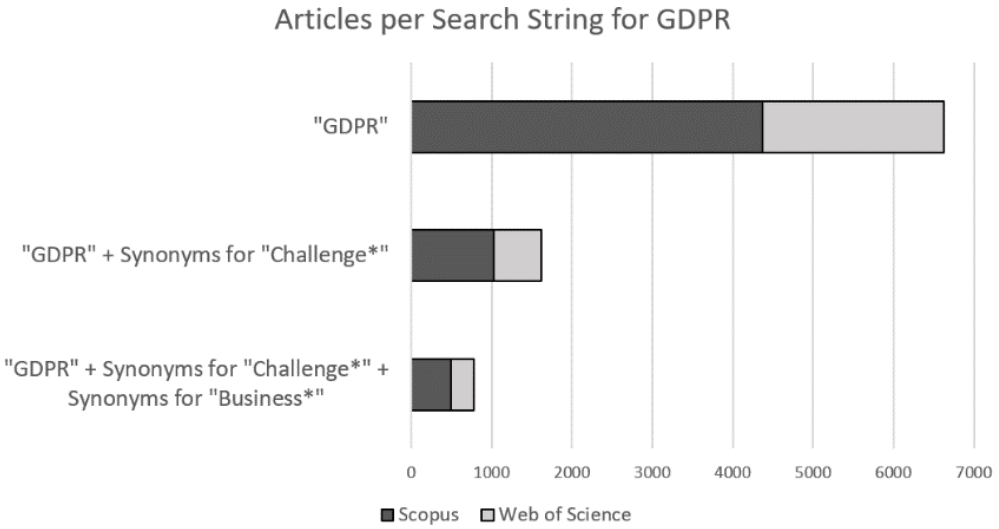

Figure 1 Articles per Search String for GDPR.

When determining the research string for the DSA, account was taken of the fact that the abbreviation DSA also has other meanings, such as Dynamic Spectrum Access, which refers to techniques for adaptive utilization of radio frequency spectrums, and Distributed Systems Architecture, which in the field of computer science refers to the design of interconnected systems. This similarity has led to many different results during searches. For this reason, the abbreviation DSA has been left out and it has been assumed that relevant studies on the subject of DSA also contain the fully written word 'Digital Services Act'. This reduced the number of search results from 3,237 to 26 for Scopus, and from 1,708 to 21 for Web of Science. This number of articles seems small but is very likely because the DSA is relatively recent. Figure 2 provides an overview of the results generated for the DSA query.

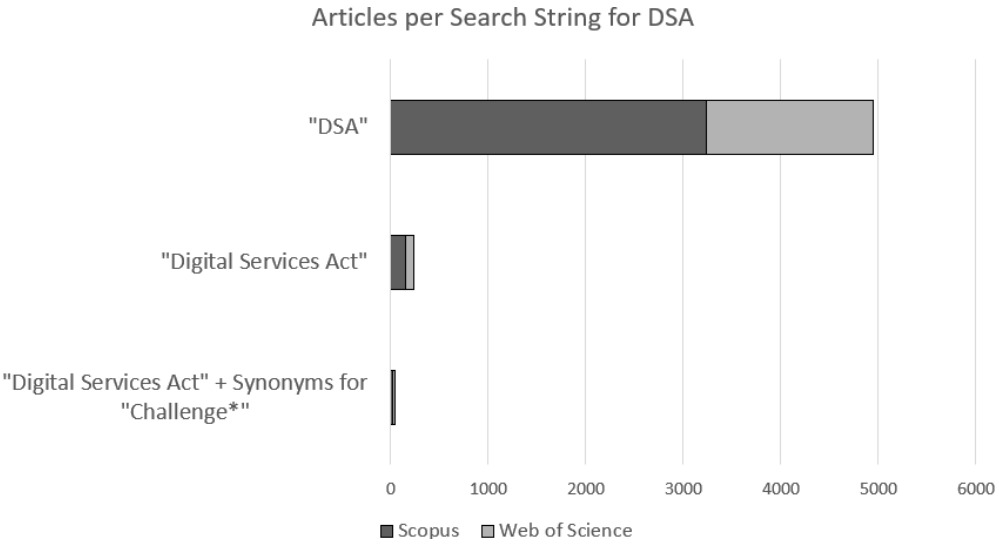

Figure 2 Articles per Search String for DSA.

3.1.3 Selection Criteria

To lessen the possibility of bias in the article selection process, selection criteria were established prior to the search procedure. To eliminate any papers that do not adhere to the requirements set for the inclusion in the review, inclusion and exclusion criteria were established. Table 5 contains these conditions. As a result, if no exclusion criterion excludes an item, those that meet the inclusion criteria are included in the review.

First and foremost, the articles must address the subjects outlined in the sub questions. For this reason, search strings were created in sub paragraph 3.1.2. Additionally, articles need to be published in scientific journals or conference proceedings. The exclusion criteria are used for filtering out any articles that do not meet the quality standard necessary for a systematic literature review. One of the reasons for leaving an article out is the publication date. The first conversations for the GDPR date from 2009 and for the DSA this is 2021. Therefore, articles from before this date are not included in the study.

Table 5 Selection Criteria for SLR.

Inclusion criteria	**Exclusion criteria**
Article includes search string for GDPR or DSA as specified in 5.2	Article is not written in English
Article is published in a scientific journal, conference paper or book	Article is not older than 2009 for GDPR and 2021 for DSA
Article presents full study, long abstracts or parts of a study are not permitted	Article does not focus on GDPR or DSA
Article is peer-reviewed	

3.1.4 Article Selection

The previous paragraphs laid out the protocol for the review of articles. The search strings for GDPR generated 777 results combined in Scopus and WOS. The results were imported to EndNote, enabling straightforward screening and selection of sources for further consideration. Removing duplicates and the first rough screening of the titles and abstracts of articles resulted in 189 articles that said something about GDPR and related challenges. After a second, more detailed, screening of selected articles, 128 articles remained. In the end, after a complete analysis for each article, 64 articles remained. These articles provide valuable perspectives on GDPR implications for organizations ranging from Small and Medium Enterprises (SMEs) to Social Media Platforms, E-commerce Platforms, IT System Providers, and Consultants, Cloud Service Providers, Cloud Computing Providers, Healthcare Institutions, Blockchain Startups, and Educational Institutions including High Schools and Universities, as well as Libraries. Figure 3 shows an overview of the literature selection method. This overview includes the different steps taken and the number of articles that were included during this review.

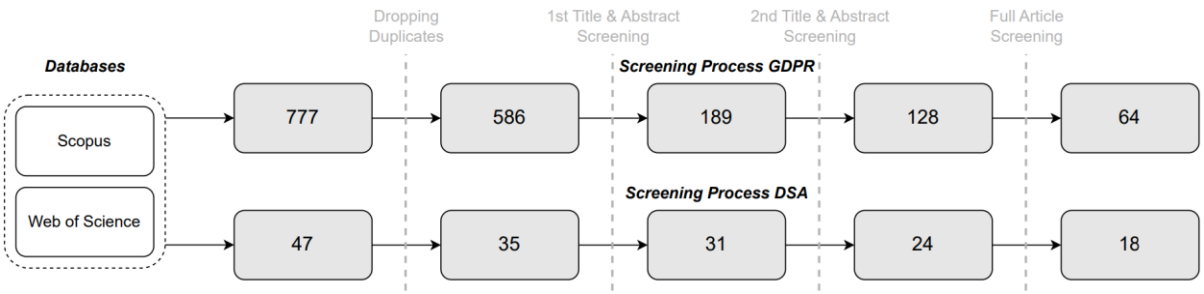

Figure 3 Overview of article screening process for GDPR and DSA.

The process outlined earlier was applied in a similar fashion for the review of articles on the DSA. Starting with an initial pool of 47 articles identified through search strings in Scopus and WOS, we began the rigorous process of refining and narrowing down this collection.

The first step involved removing duplicates, bringing the count down to 35. This was followed by an initial screening of titles and abstracts, which further reduced the number to 31 articles relevant to the DSA and its various aspects. A second, more detailed screening of these titles and abstracts was conducted, resulting in a refined list of 24 articles. The final and most thorough phase involved a complete review of each of these articles. After this full article screening, the number of articles that remained stood at 18. These articles provided in-depth insights into the implications and challenges of the DSA. They encompassed a broad range of topics and perspectives, covering content moderation, the use of algorithms, and other expected challenges for online platforms and regulatory bodies and policymakers themselves. An overview of the article screening process can be found in figure 3.

3.2 Data Synthesis

In this paragraph, we delve into the theoretical insights gained from systematic literature reviews concerning both the GDPR and DSA. The first section is dedicated to examining the various challenges organizations have encountered in adhering to the GDPR's requirements.

The latter part shifts focus to the DSA, providing a discussion on the anticipated challenges that literature predicts organizations will face in their efforts to comply with this new regulation. This section not only covers the hurdles expected at the organizational level, but also extends to the difficulties faced by the European Union and its policymakers while creating, implementing, and enforcing such a law.

3.2.1 Challenges in Literature for Complying with GDPR

Our literature review initially revealed more than 30 challenges that companies experience in pursuing GDPR compliance, but after careful selection and merging, 14 challenges remain that are mentioned in more than 5 different articles. Due to the large number of identified articles, challenges with fewer than 5 mentions are not discussed in this study and can be found in Appendix C.

While screening GDPR related articles, a previously conducted literature review on the implications of GDPR compliance for organizations surfaced. The article titled 'A systematic study on the impact of GDPR compliance on Organizations' by Machado et al. (2023), [22], delves into the effects of GDPR on organizations and examines literature findings regarding the implications organizations face in pursuit of GDPR compliance. The article identifies 9 distinct implications drawn from 23 different articles. The primary challenge highlighted is budget availability, followed by implications in the areas of writing clear consensus communications, international data sharing and the legislation not being clear. To avoid ambiguities, this study will not be included in our results table, instead it will be used to validate the results found from the SLR in this study.

Following a comprehensive screening of the entire set of articles, the challenges identified within them were systematically coded into a table (table 6). Open coding was initially employed to categorize the challenges, and subsequently, these codes were carefully compared with one another. Where feasible, codes have been combined into overarching umbrella codes, enhancing the synthesis of the identified challenges.

Table 6 provides a comprehensive overview of all challenges that companies experience in complying with GDPR. For the sake of providing a complete overview of literature on the GDPR, the GDPR-specific challenges, such as active consent management, can be seen in the table, but will not be further explained in this chapter. Instead, due to the focus of this thesis on the DSA, only the general

legal and operational challenges will be further explained in this section. For detailed information on GDPR-specific challenges, please refer to Appendix B.

Table 6 Overview of challenges faced by organizations mentioned while dealing with the GDPR.

Challenge	Source	Total mentions
GDPR lacks precise requirements, clarity, and is open to interpretation.	[23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58]	36
Resource scarcity, substantial implementation cost and time.	[27], [28], [29], [33], [59], [34], [35], [60], [36], [38], [39], [61], [62], [40], [41], [63], [42], [43], [64], [46], [58], [65], [66], [50], [51], [54], [55], [56], [67], [68], [49]	31
Difficulty with facilitating interoperability and portability across different systems, organizations, and countries	[33], [69], [34], [35], [70], [36], [71], [38], [68], [72], [73], [74], [75], [67], [76], [63], [52], [55], [25], [29], [24], [32], [37], [42], [47], [58], [77], [49]	28
(Active) consent (management) issues	[23], [24], [78], [79], [31], [32], [33], [80], [59], [81], [34], [70], [60], [37], [38], [39], [61], [40], [42], [82], [72], [83], [47], [65], [52], [74], [55], [30], [49]	28
Lack of awareness, understanding, knowledge and trained staff within organizations	[24], [26], [78], [79], [27], [28], [59], [60], [36], [38], [61], [68], [40], [43], [45], [46], [58], [65], [48], [50], [51], [55], [56], [66], [67]	25
Lack of (practical) guidance and provided standard frameworks by authorities	[23], [84], [27], [29], [35], [36], [40], [44], [45], [46], [83], [47], [65], [48], [49], [50], [51], [52], [56], [42]	20
Difficulty with operational adaption to PBD, access & authorization management, and business continuity	[23], [29], [33], [38], [39], [63], [44], [83], [77], [52], [55], [56], [24], [78], [49], [85], [76]	17
Difficulty with anonymization, pseudonymization, and encryption of data	[23], [25], [26], [29], [33], [80], [34], [38], [39], [61], [57], [65], [77], [55], [59], [54]	16
Lack of a metric or data management system to check for system security and GDPR compliance	[23], [78], [70], [40], [44], [77], [48], [76], [85], [55], [39]	11
Extensive complexity for controllers and processors outside the EU dealing with multiple regulations	[78], [31], [32], [59], [71], [39], [62], [68], [43], [52], [75]	11
Difficulty in achieving a holistic view of data and an inventory of processing actions	[29], [30], [35], [60], [38], [68], [63], [42], [43], [48], [55]	11
Difficulty of applying GDPR principles for AI and ML systems.	[23], [78], [86], [32], [69], [37], [57], [64], [76], [75]	10
Lacking data breach communication, lacking a process for timely notification of users and authorities.	[70], [60], [37], [39], [44], [82], [66], [52], [55]	9

Difficulties with DPIA (data protection impact assessment)	[79], [35], [60], [71], [38], [66], [55], [76]	8

Discussing each challenge mentioned in each article individually adds no value and also removes the function of this table. For this reason, only articles that provide the best examples or offer new and distinct perspectives are cited.

1) GDPR lacks precise requirements, clarity, and is open to interpretation.

The most mentioned challenge organizations experience while trying to comply with the GDPR is the fact that GDPR lacks precise requirements, clarity, and is open to interpretation. This poses significant challenges for organizations in various sectors trying to ensure compliance.

Almeida et al. (2022), Altorbaq et al. (2018), and Garrison & Hamilton (2019) highlight the lack of specific requirements in the GDPR. Almeida et al. (2022) note that GDPR lacks precise guidelines on obtaining free and informed consent, leading to potential abuses. Altorbaq et al. (2018) point out general ambiguity in GDPR requirements, while Garrison & Hamilton (2019) discuss the complexity and length of the regulation, leading to difficulties in interpretation and implementation.

Bampoulidis et al. (2020) and Lakshmi et al. (2020) specifically mention the need for more detailed guidelines in certain areas. Bampoulidis et al. (2020) focus on the lack of detailed guidelines for anonymizing datasets, and Lakshmi et al. (2020) emphasize the absence of guidance on effective data de-identification schemes.

Da Conceição Freitas & da Silva (2022) and Urban et al. (2019) add to this by emphasizing the need for clear, practical guides and unified guidelines. Da Conceição Freitas & da Silva (2022) stress the necessity of guides with accessible language for SMEs, and Urban et al. (2019) express a desire for more unified guidelines on handling access requests.

De Carvalho et al. (2020), Mangini et al. (2020), and Martins et al. (2020) discuss challenges related to the interpretation of specific GDPR-aspects. De Carvalho et al. (2020) note the open interpretation of legal language and requirements, Mangini et al. (2020) talk about the lack of precise instructions for data deletion, and Martins et al. (2020) state the absence of standard documents and processes.

Usman et al. (2020) and Georgiou & Lambrinoudakis (2020b) describe challenges in interpreting compliance requirements in specific contexts. Usman et al. (2020) highlights the difficulties in translating abstract compliance requirements into specific product contexts and managing trade-offs and conflicts between different requirements. And Georgiou & Lambrinoudakis (2020b) note the slow pace of GDPR compliance due to its complexity and the introduction of principles rather than concrete rules.

In conclusion, the lack of precise requirements, clarity, and the open-ended nature of the GDPR poses a big challenge for organizations. This ambiguity leads to difficulties in interpretation and implementation, especially in specific areas like consent, data anonymization, and the handling of data access requests. Addressing these challenges requires more detailed guidelines and clearer interpretation of the regulation to facilitate effective compliance.

2) Resource scarcity, substantial implementation cost and time.

The challenge of resource scarcity, significant implementation costs and time required for GDPR compliance is present for every organization, but especially for small and medium-sized enterprises (SMEs). This challenge entails financial constraints, limited human resources and the need for specialized expertise.

De Carvalho et al. (2020) and Layton & Elaluf-Calderwood (2019) emphasize that while larger companies may have the means to invest in compliance efforts, SMEs often struggle due to budget and expertise limitations. This disparity affects smaller businesses' ability to meet GDPR requirements, creating a potential gap in compliance capabilities between large organizations and their smaller counterparts. Da Conceição Freitas & da Silva (2022), in addition, highlight that SMEs, which comprise over 95% of the business world, face difficulties in complying with GDPR due to limited financial assets and human resources. Achieving GDPR compliance is described as both time and cost-consuming, impacting SMEs' operational processes.

Mangini et al. (2020) discuss the technical challenges in fully complying with specific GDPR requirements, such as the right to be forgotten. The article notes that some organizations, due to financial constraints, cannot afford significant investments in research and technical solutions needed for compliance.

Tziogas (2019) mentions that GDPR compliance can entail significant costs for businesses, potentially requiring budget increases. This suggests that the financial impact of GDPR compliance is a widespread concern for organizations across different sectors. Rossi et al. (2022) add to this that not all organizations, particularly academic ones, have sufficient in-house resources to determine and implement appropriate ethics and data protection measures. This further underscores the challenges faced by various types of organizations in allocating the necessary resources for GDPR compliance.

In summary, while the challenges around resource scarcity, substantial implementation cost, and time are present for every organization they are particularly pronounced for SMEs and certain other organizations like academic institutions. These challenges affect the ability of these organizations to effectively implement necessary GDPR measures.

3) Lack of awareness, understanding, knowledge and trained staff within organizations.

Another often named challenge is the of lack of awareness, understanding, knowledge, and trained staff within organizations.

A common theme across many studies, such as those by Bouçanova et al. (2020), da Conceição Freitas & da Silva (2022), de Carvalho et al. (2020), and Pedroso et al. (2021), is the lack of awareness and understanding of GDPR, particularly in small and medium-sized enterprises (SMEs). This lack of awareness is often attributed to the complexity of GDPR mandates and the lack clear guidance for smaller entities. In countries like Portugal and Spain, SMEs struggle with adapting to new requirements due to unskilled human resources and low academic levels, which contribute significantly to the difficulty of understanding and implementing GDPR.

The issue of training is highlighted in studies by Bouçanova et al. (2020), Li (2022), Lopes & Oliveira (2018), and Jantti (2020). These studies emphasize the crucial need for GDPR-specific training for employees to enhance their understanding of privacy requirements. There is a noted gap in preparing staff for GDPR implementation, with many organizations yet to start or complete necessary training sessions, even during the GDPR's two-year transitional period. This lack of training leads to difficulties in identifying privacy problems, interpreting GDPR regulations, and implementing compliance measures.

Mansfield-Devine (2016) and Waidelich & Schuster (2023) point out that while awareness of GDPR has improved over time, significant shortcomings remain. Some organizations, especially smaller firms, may still be unaware of GDPR's applicability to them, underestimate the potential impact of GDPR fines, or harbour misconceptions about its relevance. This is particularly true for parts of the workforce that remain uninformed about the regulations.

In conclusion, this lack of understanding and awareness impacts the ability of organizations to effectively comply with the regulation. This challenge is particularly pronounced in SMEs and in certain geographic areas where resources and expertise are limited. Addressing this challenge involves not just providing training and clear guidance but also creating a broader organizational culture of privacy awareness and compliance. This is essential for the successful implementation of GDPR and for ensuring the protection of personal data within these organizations.

4) Lack of (practical) guidance and provided standard frameworks by authorities.

In addition to the lack of precise requirements and clarity, articles also explicitly mention the lack of practical guidelines and standard frameworks provided by authorities.

One common issue highlighted by Bampoulidis et al. (2020), Lakshmi et al. (2020), and Manescu (2021) is the lack of detailed guidelines on specific aspects of data protection, such as anonymizing datasets, data de-identification schemes, and calibrating profiling based on discriminatory criteria. While authorities like the Article 29 Working Party provide some guidelines, there is a notable gap in specific and practical guidance that balances privacy and utility, particularly on a case-by-case basis.

The need for practical, tailored guidance is echoed by Cochrane et al. (2020), da Conceição Freitas & da Silva (2022), and Politou et al. (2018). SMEs express a need for more practical guidance adapted to their specific needs, including templates and guides with accessible language, considering that employees in some regions may not have sufficient English knowledge. This includes a demand for low-level implementation guidelines and business-wide requirements modelling to achieve demonstrable compliance.

Garrison & Hamilton (2019) and Urban et al. (2019) highlight the challenges in interpreting GDPR provisions like large-scale processing, access requests, and behavioural advertising due to the lack of clarity and unified guidelines. This creates challenges in assessing compliance and handling specific rights such as the "right to be forgotten" (Art. 17), as pointed out by Mangini et al. (2020), where organizations face hurdles in implementation due to few guidelines.

Marotta & Madnick (2021) and Georgiou & Lambrinoudakis (2020b) address the challenges related to data availability, storage, and the cost implications of meeting GDPR obligations, such as Article 30 - Records of processing activities. There is a noted absence of guidance on securely storing information and the high data storage costs associated with compliance.

Hirvonen (2023) specifically requests industry-specific checklists, guidance on the implementation of e-privacy regulation, formation of data protection organizations, and tools for impact assessment. This reflects a broader need for industry-tailored guidance that can aid in the practical application of GDPR provisions.

In conclusion, the lack of practical guidance and standard frameworks from authorities presents a widespread challenge in GDPR compliance. This issue predominantly affects SMEs and spans across different GDPR provisions, from data anonymization to the right to be forgotten. Addressing this challenge involves providing more detailed, specific, and accessible guidelines tailored to various industries and organizational contexts.

5) Extensive complexity for controllers and processors outside the EU dealing with multiple regulations.

Another challenge named in different articles is the extensive complexity faced by controllers and processors outside the European Union (EU) dealing with multiple regulations. This complexity arises

from managing external partnerships, data-sharing agreements, interactions with data subjects, and complying with diverse data protection laws across different jurisdictions.

Grundstrom et al. (2019), de Carvalho et al. (2020), and Lioudakis et al. (2020) highlight the challenges organizations face in managing relationships with external entities, such as third parties and data subjects. This includes the difficulties in negotiating contracts with processors for compliance, which can be both difficult and time-consuming. Handling data-sharing agreements with external entities and addressing data subject requests and rights effectively adds another layer of complexity to the operational processes of these organizations.

Garrison & Hamilton (2019) and H. Li et al. (2019) emphasize the particular challenges faced by multinational companies. Complying with multiple data protection regulations is a significant hurdle, as requirements can vary substantially across different jurisdictions. This necessitates the establishment of robust compliance programs that take into account diverse regulatory landscapes. Organizations must stay informed about changes in laws across various countries and adapt their internal policies accordingly.

Pathak et al. (2023) point out the specific challenges for organizations, including those in the Fintech and IT sectors, that store and transfer personal data outside the European Economic Area. The complexity increases when data is stored in areas where GDPR is not implemented, requiring these organizations to navigate a patchwork of different data protection laws and regulations.

The above-named challenges involve not only managing external partnerships and data-sharing agreements but also complying with a diverse range of data protection laws. This necessitates a comprehensive approach to reach compliance, involving contract negotiations, effective handling of data subject interactions, and the adaptation of internal policies to meet varied regulatory requirements across different jurisdictions.

6) Difficulty in achieving a holistic view of data and an inventory of processing actions.

With 11 mentions, the challenge of achieving a holistic view of data and maintaining an inventory of processing actions is another hurdle for organizations striving for GDPR compliance. This challenge encompasses developing an understanding of all data processing activities, including the categories of data, data subjects, and the purposes of processing.

Both de Carvalho et al. (2020) and DePaula et al. (2018) emphasize the difficulties organizations face in gaining a holistic view of the data they process and maintaining a thorough inventory of processing actions. This involves understanding every aspect of data handling within the organization, a task that is crucial for adhering to GDPR requirements.

Additionally, H. Li et al. (2019) and Lioudakis et al. (2020) highlight the specific challenge in developing and maintaining effective tools and systems to manage this data. Implementing holistic search tools and creating comprehensive data views are essential for organizations to monitor and manage their data processing activities effectively.

Labadie & Legner (2023) highlight the significant effort required in maintaining records of processing activities and system landscape documentation. This challenge is worsened by the large number of systems and processing activities typical in organizations. Documentation becomes a complex task, requiring great attention to detail and a balanced approach.

The difficulty in achieving a holistic view of data and maintaining an inventory of processing actions is significant in reaching GDPR compliance. It requires organizations to develop thorough understandings

of their data processing activities, implement holistic search tools, and maintain detailed records and documentation.

3.2.2 Conclusion of GDPR Challenges

The challenges identified in GDPR compliance, such as ambiguities in requirements, limited resources, lack of clear guidance and gaining visibility over internal processes, shed light on widespread issues within the digital regulatory landscape. These issues underscore the significant barriers to achieving compliance, highlighting the need for unambiguous regulations, adequate resources, and deep organizational insight and training.

Revisiting the similar study introduced in paragraph 4.2.1, our SLR closely aligns with the conclusions drawn in “A systematic review of the impact of GDPR compliance on organizations” by Machado et al. (2023). It highlights similar challenges faced by organizations under GDPR mandates. While there are differences in the order and number of articles reviewed, the core issues remain consistent, with the lack of clear requirements, guidance, resources, and knowledge under GDPR proving to be the most significant challenges. This validation not only strengthens the credibility of our SLR results but also underscores the widespread nature of these challenges across studies.

Given our understanding of the challenges posed by the GDPR, we can expect that companies may face similar challenges under the DSA, including the need for clarity in regulatory requirements, sufficient and appropriate allocation of resources and obtaining internal expertise to manage compliance. This parallel suggests a crucial need for clear guidance and practical frameworks, elements that have proven essential in navigating the GDPR and are likely to be equally crucial for DSA compliance. Furthermore, the GDPR's emphasis on developing a compliance-oriented organizational culture highlights a strategy for successfully adapting to and managing the new regulatory requirements posed by the DSA.

These insights are not just academic, they have practical implications for the next phases of this research. As we prepare to interview experts, understanding these challenges allows us to ask targeted questions and explore areas, particularly around operational strategies and organizational adjustments needed for compliance. What remains unclear, and what we need to delve deeper into, are the specific operational nuances and best practices that can mitigate these anticipated challenges under the DSA.

Therefore, the expert interviews will aim not only to confirm known challenges, but also to uncover actionable insights and practical recommendations to effectively navigate the DSA requirements. This approach will allow us to build a comprehensive understanding of the regulatory landscape, giving stakeholders the knowledge to proactively address future regulations.

3.2.3 Challenges in Literature for Complying with the DSA

With the DSA being a relatively recent development in the European Union's regulatory framework, academic literature has shown limited experiential analysis in the field of compliance challenges. As of August 2023, only the first 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) were required to adhere to the extensive obligations set forth by the DSA. Therefore, most of the literature available primarily evaluates the Act itself, speculating on potential challenges and areas of concern, rather than providing practical insights from direct experiences. Some other papers performed comparisons with existing national legislations, such as Germany's NetzDG and Austria's legal framework aimed at combating online hate speech. These comparative studies highlight the similarities and differences in approach. Other research papers delve into the challenges faced by the European Union and its policymakers in creating, implementing, and enforcing such a comprehensive regulation.

After analysing all papers, partly due to these different perspectives, it was decided to divide the 'expected' challenges into two tables. One explaining the expected challenges that companies will likely experience (Table 7) and the other elaborating on those that the EU and its policymakers experience when creating, implementing, and enforcing the DSA (Table 8). In the following paragraphs, we will discuss all found categories and associated challenges for each table.

In the academic research environment, articles often deal with highly specialized topics. However, this specificity may hinder the synthesis of insights from different articles or even the application of their findings to broader, global contexts. Despite this, an attempt has been made to merge and generalize challenges, therefore it must be taken into account that this may have introduced bias and that displayed challenges might not fully correspond to what was said in the papers.

Challenges faced by organizations while trying to comply with the DSA

The following table shows the challenges found in literature that organizations experience while trying to comply with the DSA. Each challenge will be discussed below the table.

Table 7 Overview of challenges faced by organizations while dealing with the DSA.

Category	Challenge	Source	Total mentions
Legal complexity	Legal complexity of DSA and other existing laws/ complexity of the current EU legal framework, including the GDPR, DMA, and AIA, and the challenge for organizations to understand and comply with these regulations.	[87], [88], [89], [90], [91]	5
	Complexity of Procedural Rights, right to be heard, informed and to remedy.	[92]	1
	Variation in national laws like NetzDG in Germany, and a law against online hate in Austria.	[92]	1
	No clear guidelines on Influencer marketing as it typically falls outside the DSA's definition of advertising.	[93]	1
	The absence of clear guidelines in the DSA for distinguishing parody from copyright infringement, leading to potential legal uncertainties for content creators and platforms.	[94]	1
Content moderation and freedom of expression	Complexity of content moderation and the challenges platforms face in balancing the removal of harmful content with freedom of expression and information and across different regions.	[92], [95] [96], [97], [98], [99]	6
	Ambiguity around the limitations of algorithmic content moderation, including potential over- or under-removal of content. And the challenge of ensuring algorithmic accountability and transparency.	[88], [96], [94], [99]	4
	Interpretation and application of what is illegal or harmful can be subjective.	[92]	1
	Moderating coded communications such as memes, which often use humour and ambiguity, making it hard to identify and regulate hate speech or radicalization.	[96]	1

	The evolving nature of online speech and how hate speech and radicalization tactics adapt over time, presenting ongoing challenges for compliance with the DSA.	[96]	1
	The complex nature of assessing whether a piece of content is a legitimate parody, which requires nuanced understanding beyond the capabilities of current algorithmic tools.	[94]	1
Operational and resource challenges	Organizations need to adapt their business practices to ensure compliance with regulations, balancing commercial interests with legal obligations.	[87], [88]	2
	Alternative dispute mechanisms require new processes and systems which are resource intensive.	[92]	1
Data privacy	Ensuring adequate consumer protection and data privacy within the scope of the DSA and protecting privacy in the age of big data, where user tracking and profiling are common practices.	[100], [96], [89], [97]	4
Technological evolution and its impact	Evolving business models and advertising practices may require continuous adaptation to stay compliant with evolving regulations.	[101], [93]	2
	Ensuring transparency and accountability in the use of Hypernudging techniques poses a significant challenge, particularly given their opaque and complex nature.	[90]	1
	No clear definition for freedom of thought and balancing the right to freedom of thought with the rapid development of emerging technologies, especially AI and neurotechnology, that may impact this fundamental right.	[102]	1

1) Legal complexity

One of the challenges that emerged when analysing the articles was legal complexity. One of the reasons for this complexity stems from the fact that the DSA doesn't exist in isolation. It intersects with other intricate EU laws like the GDPR, the DMA and AIA, which cover data protection, digital markets, and artificial intelligence.

Papers from Đurović & Kniepkamp (2022), Greif & Grosz (2023) and Hacker (2021) have pointed out that this mix of laws creates a tricky landscape for companies, especially when dealing with specific online areas like reviews or job ads. Each of these laws has its own set of rules and requirements, and companies must figure out how to follow all of them at once, which is no small task.

Then there's the aspect of fairness and procedural rights, discussed by Bayer (2022). When companies moderate content on their platforms, they need to ensure they're not just compliant with these laws but also fair in how they treat users' rights to be heard or to appeal decisions. This becomes even more complex when you consider that laws vary from country to country, like Germany's NetzDG or similar laws like the one in Austria, making it hard for companies that operate internationally to stay consistent.

Specific issues add to this complexity. For instance, the regulation of influencer marketing, as highlighted by Duivenvoorde & Goanta (2023), falls into a grey area under the DSA. Also, distinguishing

between what's considered a parody and what's a copyright infringement is not defined in the DSA, as noted by Pakutinskas & Šepetys (2023). This lack of clarity can lead to potential legal uncertainties for content creators and platforms.

The challenges are significant because they directly affect how well organizations can understand and comply with the DSA in conjunction with other EU laws. It's a complex balancing act that requires careful navigation to avoid legal pitfalls while trying to operate effectively in the digital space.

2) Content moderation and freedom of expression

Finding a balance between content moderation and freedom of expression appears to be another challenge for digital platforms, primarily revolving around the delicate balance between removing harmful content and respecting freedom of expression.

Bayer (2022), Kucina & Univ Latvia (2022) and Reviglio & Santoni (2023) address the difficulty of this balancing act. They point out that platforms are in a tough spot when it comes to deciding what content to remove. On one hand, they need to keep illegal or harmful content off their platforms to ensure a safe online environment. On the other, they have to be careful not to infringe on people's freedom of expression, which is a cornerstone of democratic societies. This is no easy task, as what constitutes harmful or illegal content can often be subjective, as highlighted by Bayer (2022) again, adding another layer of complexity to this issue.

Mazúr & Grambličková (2023) contribute to this conversation by emphasizing the need for independent and effective content moderation mechanisms. They note that even before the DSA's implementation, models like Meta's Oversight Board struggled to balance content moderation with freedom of speech. Additionally, they recognize some elements of judicial independence in these models but state that these need further improvements for them to be more effective.

Mezei & Szentgáli-Tóth (2023) mention the challenge of regulating online platforms in a way that prevents misinformation and cyber-attacks, while also safeguarding freedom of expression and democratic discourse. They note that this is particularly relevant in our era of 'fake news' and online manipulation.

Farrand (2023) brings up several points: the difficulty in moderating coded communications like memes, which often straddle the line between humour and potentially harmful content. The limitations of algorithmic content moderation, which might lead to either over-removal or under-removal of content. And the evolving nature of online speech, with hate speech and radicalization tactics constantly changing, making it hard to keep up with effective moderation.

Lastly, Pakutinskas & Šepetys (2023) discusses the specific challenge of using algorithmic tools to identify parody content. Parodies often require a nuanced understanding to differentiate them from infringing content, and current algorithms or tools might not be sophisticated enough, leading to potential over-blocking of legitimate content.

So, while these named papers delve into quite specific details, they collectively underscore one challenge: the difficulty of finding a balance between content moderation and freedom of expression. This balancing act is complex because it involves interpreting subjective content, determining the line where freedom of speech becomes harmful expression, and adapting to the evolving nature of online communication. And with this, online platforms face the task of creating policies that are both effective in limiting harmful content and respectful of the different perspectives that make up an online community. What makes this challenge significant is that these decisions directly influence the quality of online content and the protection of individual rights. Mistakes here can lead to either a stifling of

free expression or a proliferation of harmful content, both of which can have big implications for society. Therefore, these challenges are not just operational concerns for platforms but are also important in shaping the digital landscape and preserving the values we have in our society.

3) Operational and resource challenges

Another challenge that emerged from the articles are operational and resource challenges. These primarily focus on adapting business practices and developing new systems to comply with regulatory requirements.

Đurović & Kniepkamp (2022) highlight the need for organizations to modify their business practices, particularly in the context of online reviews. This involves not just aligning with the legal obligations but also maintaining a balance with commercial interests. These adaptations could range from changing how reviews are collected and displayed to ensuring transparency and fairness in review management, all while keeping an eye on business profitability.

Greif & Grosz (2023) discuss the technical and operational challenges that arise when implementing specific legal requirements. They state that the DSA requires platforms to develop and integrate new solutions that are compliant with legal standards, which can be a complex and resource-intensive process. It's not just about tweaking existing systems; it often involves overhauling or building entirely new functionalities to meet these regulatory needs.

Bayer (2022) describes the use of an Alternative Dispute Resolution (ADR). They note its introduction as a significant operational change for platforms. ADR mechanisms, designed to provide efficient, fast, and cost-effective solutions in disputes related to online content, require platforms to develop new processes and systems. This demands quite a few resources, both in terms of technology and human expertise. The goal here is to bring justice closer to the origin of the problem and alleviate the burden on courts. However, setting up such mechanisms means platforms must invest in creating infrastructures that can handle dispute resolution effectively, often requiring a rethinking of current operational models.

These operational and resource challenges directly impact the ability of organizations to comply with the DSA while maintaining their operational efficiency and business interests. Adapting business practices, implementing new technical solutions, and establishing ADR mechanisms are resource intensive tasks that require significant investment and strategic planning.

4) Data privacy

Dumancic (2021) highlights the challenge of ensuring proper consumer protection and data privacy under the DSA. This means that platforms must not only protect user data, but also ensure that their data handling practices are transparent and meet strict privacy standards. This task is complex, given the enormous amounts of data these platforms process on a daily basis.

Hacker (2021) emphasizes the need for an integrated approach to address algorithmic manipulation. And hereby points out that aspects of unfair commercial practices, data protection and privacy legislation are intertwined. The article argues that the DSA is ambitious but in its current form does not go far enough to fully address the nuances of algorithmic manipulation. And emphasizes that this is especially not the case for smaller digital services and direct marketing by smaller platforms. It points out that the DSA's main focus is on transparency and risk management for large platforms, leaving gaps in coverage.

Kucina & Univ Latvia (2022) highlight the risks associated with collecting and processing big data. They highlight how platforms' business models can infringe on individual privacy and manipulate user

behaviour. This raises significant concerns in the context of the DSA, which is primarily concerned with removing illegal content and places much of the responsibility on online platforms.

In addition, the authors point to the European Commission's hesitation, possibly due to lobbying influences, to impose strict rules on profiling and microtargeting. Such practices, as criticized in the text, invade privacy and manipulate behaviour. However, the article does acknowledge that the DSA and DMA have taken steps toward addressing issues of surveillance, profiling and microtargeting, especially for large platforms. Mainly by mandating transparency in the use of recommendation systems and offering more control to users.

These data privacy challenges are challenging due to the massive amounts of data being processed and the need to prevent algorithmic manipulation. The DSA's current focus on large platforms and transparency mainly leaves gaps for smaller services. The European Commission's cautious approach to profiling and microtargeting also plays a role in this. Finding this balance is not only crucial for operational effectiveness, but also for maintaining user trust.

5) Technological evolution and its impact

The identified challenge technological evolution and its impact includes challenges caused by advancing technology, especially in the areas of advertising and manipulation of user behaviour.

Alminen et al. (2022) discuss how evolving business models and advertising practices, driven by technological advances, require continuous adaptation of online platforms to remain compliant with changing regulations. This goes both ways as both the technology and regulatory landscape are in flux.

Duivenvoorde & Goanta (2023) highlight a specific challenge with hybrid advertisements, which are increasingly common in influencer marketing. These ads, which blur the lines between content and advertising, challenge the effectiveness of the DSA. As platforms introduce new forms of monetization, such as influencer marketing, they generate content that often masquerades as authentic, bypassing traditional advertising rules. The DSA's exclusion of influencer marketing from its scope highlights a void in addressing these emerging advertising practices.

Morozovaite (2023) points out the challenges of ensuring transparency and accountability when using Hypernudging techniques. These techniques use big data and algorithms to subtly influence user behaviour, creating personalized environments that can lead to manipulative outcomes.

O'Callaghan et al. (2023) address the issue of freedom of thought in the context of emerging technologies such as AI and neurotechnology. They point to the lack of a clear definition of this fundamental right and the challenges in balancing it with the rapid development of these technologies, which could potentially impact it.

These challenges are significant for online platforms because they require constant adaptability. These challenges highlight the need for platforms to evolve their business models, ensuring transparency in advanced advertising and user influence techniques. And also, to protect fundamental rights in the face of technological progress.

Challenges faced by policymakers while designing and implementing DSA

Now that all ‘expected’ challenges in literature regarding online platforms are discussed, we continue with elaborating on those that the EU and its policymakers experience when creating, implementing, and enforcing the DSA. These can be found in table 8 and will be discussed below.

Table 8 Overview of challenges faced by policymakers while designing and implementing DSA.

Category	Challenge	Source	Total mentions
Regulatory harmonization and legal fragmentation	The harmonization of digital laws across EU Member States, ensuring compliance while respecting national differences, prevent regulatory competition and legal fragmentation.	[100], [103], [104], [91], [105]	5
	Transnational nature of platforms and the difficulty in applying local and transnational regulatory approaches.	[101]	1
Balancing regulation and innovation	Challenge in regulating digital platforms to ensure consumer protection and fair competition while also fostering innovation and growth in the digital sector.	[100], [105], [90]	3
Challenges in implementing and enforcing DSA	Ensuring effective enforcement and practical implementation of the DSA's provisions, especially regarding influencer marketing, undisclosed advertising, and provisions against large platforms.	[93], [89], [97]	3
	Challenge in clearly defining digital service providers and which platforms are considered VLOP's or gatekeepers, this includes balancing inclusiveness to avoid unfairly targeting or excluding certain platforms.	[100], [105], [91]	3
	Difficulty in adapting legal frameworks to the evolving nature of machine learning and AI technologies, like e.g. Hypernudging [90], ensuring that regulations like the DSA and DMA remain relevant and effective.	[89], [105], [90]	3
	complexity of regulating platform operators, who often act beyond the role of traditional intermediaries. This includes their role in content moderation and their status under the "safe harbour" liability regime.	[104]	1

1) Regulatory harmonization and legal fragmentation

Harmonizing regulations and preventing legal fragmentation is a frequently mentioned challenge for the EU and its policymakers. Several articles state that the establishment and implementation of the DSA is a step in the right direction. But they point out that it is difficult to align national legislation with EU-wide regulations, while ensuring consistency and respecting individual differences.

Dumancic (2021) and Nóra Kiss (2023) both emphasize the need for harmonization of digital laws across the EU. They note the importance of integrating the different national digital markets into one harmonized market. Nóra Kiss (2023) argues that the EU has the opportunity to influence global digital law through its regulatory power, making harmonization an instrument of soft power. However, this process is complex and requires a careful balance between the powers of countries and the EU.

Rudohradská & Trescáková (2021) and Huckova & Semanova (2022) mention the importance of consistent implementation and enforcement of the DSA and DMA in member states. They say it is essential to prevent legal fragmentation and ensure a single digital market. They describe this task as difficult due to the enormous diversity of the digital landscape and the varying levels of digital literacy and infrastructure in different regions of the EU.

Rodríguez de las Heras Ballell (2021) elaborates on the crucial nature of achieving a high level of EU harmonization to address legal fragmentation. The challenge is to avoid regulatory competition

between Member States. This could be harmful to the European digital single market. Moreover, there is the need to manage the impact of regulation on platforms outside the EU. This could lead to the EU being isolated from the rest of the world through strict rules.

The challenges of regulatory harmonization and legal fragmentation described above are of great importance to the EU and its policy makers. As it is not just about aligning different national laws within the EU, but also about ensuring that these regulations are consistent and effective in a rapidly evolving digital market. Achieving this harmonization is crucial competitive and united as Europe.

2) Balancing regulation and innovation

Another challenge that comes up in various articles is balancing regulation and innovation. This challenge involves creating regulatory frameworks that protect users and promote fair competition, without diminishing the character of digital innovation.

Dumancic (2021) and Huckova & Semanova (2022) both emphasize the difficulty of striking a balance between regulation and innovation. The often rapid change in the digital environment means that the DSA must be flexible enough not to hinder innovation. This balance is very important, as overregulation can stifle the creativity and competitiveness of the digital sector in Europe.

The rise of large digital platforms, which often act as a gateway to the digital economy, complicates this. Due to their size, these can create barriers to market access, which can lead to an unfair competitive advantage. This situation can increase the risk of things like higher prices, lower quality, less choice and hampered innovation (Huckova & Semanova, 2022).

Morozovaite (2023) adds to this discussion by highlighting the challenge of protecting users from manipulative practices such as hypernudging, which are increasingly common in digital markets. While promoting innovation is essential, there is also an urgent need to ensure that this innovation does not come at the expense of user manipulation or exploitation.

In summary, the challenge of balancing regulation and innovation for the EU and its policymakers is significant, as it directly impacts the region's ability to remain competitive and innovative in the global digital economy. Balancing this requires a nuanced approach to ensure regulations such as the DSA protect users and promote fair competition. The aim is to do this without limiting the innovative potential of the digital sector.

3) Challenges in implementing and enforcing DSA

Another challenge identified for the EU and its policymakers is the implementation and enforcement of the DSA. One of the issues we placed in this category revolves around the regulation of emerging digital advertising trends, such as hybrid advertising that blurs the lines between influencer marketing and personalized advertising. Duivenvoorde & Goanta (2023) delve into this challenge and point out the difficulty of effectively regulating these evolving practices under the DSA, especially due to their diverse and dynamic nature. They mention the enforcement of rules against undisclosed advertising, especially in the field of influencer marketing, as not or little present in the DSA.

Hacker (2021) highlights a different challenge. They argue that ensuring effective enforcement and practical implementation of the DSA's provisions against algorithmic manipulation is difficult given the rapid advancement and complexity of the underlying technologies. The solution they propose is, 'non-manipulation by design'. And this aims to proactively reduce manipulative influences, in line with data protection efforts to protect individual autonomy.

The practical implementation of the DSA, especially in terms of its scope and enforcement against large platforms, is another concern, as noted by Kucina & Univ Latvia (2022). This includes not only defining

what constitutes a digital service and distinguishing between service providers and intermediaries, but also determining which platforms will be considered VLOPs or gatekeepers, subject to the obligations of the DSA and the DMA. Dumancic (2021) and Huckova & Semanova (2022) emphasize the importance of balancing inclusivity in these definitions to avoid unfairly targeting or excluding certain platforms.

Furthermore, the rapid evolution of digital markets and technologies, especially in areas such as machine learning and AI, poses an ongoing challenge. Ensuring that regulations such as the DSA and DMA remain relevant and effective in such a rapidly changing environment is a crucial task for policymakers. This point is echoed by Morozovaite (2023), who discusses the need to adapt existing legal frameworks to effectively address the nuanced nature of hypernudging.

Finally, regulating platform operators, who often act outside the role of traditional intermediaries, is a complex issue. As Rodríguez de las Heras BalleII (2021) discusses, this also includes their role in content moderation and their status under the “safe harbour” liability regime. These platforms have significant influence in the digital space and defining their responsibilities and liabilities presents unique challenges. Especially in a modern world where digital interactions and transactions are becoming increasingly sophisticated.

Although these articles cover the topics in reasonable detail, they all boil down to one principle: the EU's multifaceted challenge in implementing and enforcing the DSA. Regulating innovative and rapidly evolving digital practices, defining the scope of digital services and gatekeepers, adapting to new technologies and managing platform operators are all crucial for ensuring a fair and competitive digital market in Europe. The difficulty lies in the dynamic nature of the digital landscape, which is constantly evolving, requiring regulators to be both flexible and forward-thinking. This balancing act requires a regulatory approach that not only responds to current digital phenomena, but also anticipates future developments. This ensures that the digital market remains a good environment for innovation, competition, and consumer protection.

3.2.4 Conclusion of DSA Challenges

As mentioned earlier, the literature on experiences surrounding the DSA is scarce and often concerns highly specialized topics. A large part of the available literature is also speculative. Nevertheless, after synthesizing and generalizing literature, several anticipated challenges have emerged.

The literature shows that online platforms must navigate a labyrinth of legal, operational, and ethical challenges to comply with the DSA. 8 of the 18 articles identify various forms of legal complexities, this concerns complexities in the DSA but often highlights its intersections with other EU laws such as GDPR, DMA and AIA, creating a dense regulatory landscape that requires simultaneous compliance.

Another challenge that is widely discussed in the literature is content moderation, again 8 out of 18 articles identifying it as a challenge. These discussions frequently focus on the difficulties online platforms face in striking a balance between removing harmful content and preserving freedom of expression. Additionally, the subjective nature of what constitutes illegal content, which can vary significantly from country to country, is also highlighted as a complicating factor.

The current literature mainly addresses these two largely legal challenges, with speculative discussion of possible intersections with other regulations and whether terms and approaches are adequately addressed in the DSA. Operational challenges, such as organizing business operations, managing resources, and addressing rapid technological evolution, are broadly discussed but less emphasized in the literature. Despite this, these challenges can significantly strain platforms, necessitating changes

in business practices, technical systems, and the adoption of new mechanisms like alternative dispute resolution.

Similarly, the SLR on GDPR compliance challenges highlights the significant role of general operational challenges in new digital regulations. Common issues include ambiguities in requirements, limited resources, challenges in obtaining a comprehensive understanding of the organization, and the necessity for thorough organizational insight and training.

Significant gaps remain in our understanding due to the existing literature being largely speculative rather than grounded in practical experience. While we know the general legal and operational challenges following these literature reviews, the specific day-to-day implications for business practices are less clear. For example, it is not sufficiently known how online platforms deal with such regulations internally, what they need and how they adapt their technical systems or business models. These areas are critical to achieving compliance and urgently require more research to develop a deeper understanding.

The DSA challenges arising from Table 7 and the general legal and operational challenges of the GDPR form the basis for the expert interviews in the next chapter. Based on their experience, these experts can provide real-world insights into effective compliance strategies, regulatory challenges, and balancing operational capabilities with regulatory obligations. The interviews delve deeper into the nuances of implementing DSA guidelines. Additionally, through these expert discussions, we hope to reveal how organizations interpret ambiguous legal texts, prioritize actions to mitigate risk, and invest in technologies and processes that support compliance in a cost-effective manner.

Although not the primary focus of this research, at the other end of the spectrum, the EC and policymakers also experience specific challenges in introducing and enforcing the DSA. These challenges encompass the difficulties of harmonizing digital law across member states, preventing legal fragmentation, balancing regulation with innovation, and ensuring effective implementation and enforcement of the DSA. While this study primarily examines online platforms, understanding these broader policy challenges can provide valuable insights into the legislative process and its operational execution. In the subsequent chapter, experts will be consulted to delve deeper into these issues, providing detailed insights on these challenges and exploring the interactions among various stakeholders, including online platforms, the EC, and auditors.

4 Results

The literature review has thoroughly examined the existing and expected challenges, thereby paving the way for the empirical phase of this study. In the first section of this chapter, we design and conduct interviews with industry professionals who specialize in digital law and the DSA. These experts have either been involved in or are currently engaged with various DSA implementation projects. Our goal is to validate the challenges identified through literature and to discover emerging issues, as well as to explore strategies for addressing them. In the subsequent part of this chapter, we translate segments from the theory and, primarily, findings from interviews into a risk mitigation framework. In this framework, we identify risks associated with different challenges and establish corresponding risk mitigation measures. This approach is aimed at providing online platforms with practical tools to enhance their compliance with the DSA and to better navigate future regulatory environments.

4.1 Developing the Semi-structured Interviews

This phase of the study encompasses gathering primary data through interviews with experts and researchers. To allow the interviewees to express their own opinion, semi-structured interviews are used. These often use guiding themes with the aim to let interviewees respond as openly as possible. They include specific questions but also allow interviewees to let his or her own perspectives shine through [106], [107]. When conducting the semi-structured interviews, the methodological strategy of Adeoye-Olatunde and Olenik (2021), [10], is used. Table 9 displays the seven processes they outline for conducting, analysing, and reporting data from semi-structured interviews, along with the subtopics that need to be covered. The authors note that although the methodology was initially developed for pharmaceutical services research, it can be used for a variety of research projects.

Table 9 Seven steps to conducting, analysing, and reporting semi-structured interview data [10].

Steps	**Sup-topics**
1. Assess appropriateness of the semi-structured interview: best method to address research objective(s)?	None
2. Sampling and participant recruitment	2a. Sampling approaches 2b. Recruitment
3. Data collection design	3a. Developing the semi-structured interview guide 3b. Collecting participant demographic information
4. Conducting the interview, transcription, and data transmission and storage	4a. Preparation and training 4b. Interview modality and recording considerations 4c. Transcription and checking 4d. Securely storing and transmitting data
5. Data analysis	5a. Coding and theme identification 5b. Establishing rigor
6. Drawing conclusions	None
7. Reporting results	7a. Reporting guidelines 7b. Data display

Recruitment of participants and sampling are the focus of step 2. For the sampling of the interviews, we use a mix between purposeful sampling, where we explicitly look for participants that possess certain traits or qualities, e.g., experts and researchers in the field of digital regulation, and snowball sampling, where we try to expand the sample by asking each participant to recommend other potential participants. We conclude the data collection when saturation is reached, according to Saunders et al. (2017), [108], this happens when the researcher begins to hear the same comments repeatedly. It is then time to stop collecting data and start analysing what has been collected.

Step 3 focuses on the design of the data collection. Appendix D includes participant preferences, outlines the demographic data collected, and provides the interview guide. From each participant, the following information is collected to create a profile while maintaining their anonymity: title of employment, years of experience, industry in which the company operates, and number of employees.

The 4th step addresses issues with data recording and storage. Microsoft Teams is used to conduct video calls for the interviews. Every interview is recorded. The recordings are only kept locally and after being processed, they are erased. Due to the confidentiality obligations of various participants, elements that could identify companies or individuals are anonymized. All transcripts can be found in Appendix E. Some of these transcripts are in Dutch, while others are in English.

To find patterns and distinctions in the interview results, one of the last steps of this methodological approach involves transcribing and coding the audio recordings of the interviews. For transcriptions, we use the automated transcription software of Microsoft Teams, after which we check and correct possible errors. For the coding of the interviews, we export transcriptions to ATLAS.ti 24, which is a renowned coding software. Given the exploratory nature of this research, we employ an inductive coding technique to reveal overarching themes within the interviews. This method allows us to draw conclusions, effectively highlight key findings, and directly address the primary research question.

4.2 Data Analysis

This section begins with an analysis of the interview outcomes to determine if the data collected allows us to draw conclusions that enhance our understanding of the challenges faced by online platforms in complying with the DSA. The structure of this section is guided by the overarching themes identified during the coding process. We will first offer a detailed exploration of all interview results, emphasizing the various nuances involved. Following this, we will conduct a detailed analysis of these findings, stating the importance of each challenge. These findings will then be compared with the theoretical insights from the SLRs. This comprehensive analysis ultimately leads to translating the findings into a risk mitigation framework, designed to address the identified challenges.

1) Openness to interpretation and lack of guidance

The Digital Services Act poses significant challenges to online platforms, for example, due to its openness to interpretation and lack of clear guidelines. These issues are compounded by the presence of vague terms and open standards within the DSA, leading to uncertainty in complying with the legislation. Specific examples, such as the varying composition of definitions such as "diligent, objective, proportionate" and the lack of specification for terms like "timely" and "significant change", illustrate the difficulty of interpretation and the need for companies and auditors to give meaning to these terms themselves.

The lack of concrete guidance following the introduction of the DSA causes frustration. It is noted that "almost two years later", there is still a lack of specific guidance. This lack of guidance, together with the suggestion that additional guidance would follow, as was the case with the guidance provided to the GDPR by Working Party 29, leaves a lot of room for companies' own interpretation. It is also mentioned that current guidance by the EC, for example in the form of a Q&A, is inadequate for practical implementation. As one participant puts it: "You can't say, hey, this is guidance you can really use as an organisation". The lack of this guidance and room for interpretation leads to situations where companies tend to interpret the law to their advantage: "You see that tech companies often choose the narrowest possible definition; this is often at the expense of the spirit of the law."

The complexity of the DSA is further highlighted by interpretation problems caused by the difference in perspective between lawyers who write the law, the companies that must comply with it, and the

auditors who must test it. This leads to 'lost in translation' moments. Moreover, the diversity of online platforms, such as social media versus booking sites, adds to the complexity, with the DSA seeming to take a "one size fits all" approach.

A specific challenge frequently mentioned is the protection of minors, for which the DSA sets targets without clear guidance on implementation. This forces companies to make their own decisions on how to meet these requirements based on risk assessments, raising questions as to whether interpretations match EU expectations.

In summary, the cited experiences underline the significant challenges online platforms face under the DSA. The need for companies to interpret vague terms themselves and the absence of specific guidance lead to uncertainty and potential risks for both compliance and regulatory effectiveness. This highlights the importance of developing more specific guidelines and definitions to facilitate and clarify the implementation of the DSA.

2) Lack of audit standards

The openness to interpretation and lack of standards are also evident in the delegated act for auditors. It is mentioned that this guidance does outline some sort of prerequisites, but it is considered a very "strange" law. One participant states: "You can clearly see that at one point people with IT audit knowledge were involved in writing it, but they were not involved to the end. So, there are weird inconsistencies in it, and it doesn't refer to existing auditing standards."

It is mentioned by a participant that there are significant differences in Transparency Reports between companies, as well as in risk control matrices, and the conduct of systemic risk assessments. She stresses that this need not be a problem, if it is audited uniformly to some extent, if not "one audit opinion is not worth the other". This indicates there is a distinct lack of standards, and this is already evident in practice.

Although there are working groups with stakeholders, discussing the need to fill in open standards, a shared framework is not yet visible. This leads to uncertainty among auditors about how to effectively audit the DSA, and uncertainty among online platforms about how they should deal with these audits in the future.

Auditors and companies are in discussions at the European level to develop some kind of audit standard, but so far without adoption by the European Commission. These discussions seek to create some form of uniformity in audits, to avoid the value of audit opinions varying due to different interpretations and approaches. The Big Four agree that ISAE 3000 is the best fit, "Only it does not align with the delegated act brought out by the EU." Ultimately, auditors and companies were able to comment on this delegated act, but, emphasises one participant, "you then actually see that nothing has been done with those comments".

In summary, this illustrates the challenges auditors face when auditing online platforms' compliance with the DSA. The lack of standardised frameworks and clear guidelines leads to variability in audit practice and raises the need for further development of industry standards and uniform approaches. The efforts of the Big Four, online platforms, and the European Commission are crucial in seeking greater clarity and consistency in future DSA audits.

3) Audit reports and time constraints

Another topic that frequently emerges in the interviews is the requirement for VLOPS to undergo audits for reasonable assurance and operating effectiveness in the first year the legislation is enforced, instead of limited assurance or just design and implementation. This is described as "unique" and

"asking a lot in the first year". It is also mentioned that this is a type two where it concerns a period rather than a point in time.

This high requirement for assurance combined with the fact that additional guidance for audits (20 October 2023) came out later than the controls should have been "in place" makes all participants suspect that not many of the audit reports will be positive. Participants also emphasize that many platforms, especially VLOPS, experience time pressure and that "in a lot of cases the processes are in place, but they do not have audit evidence to show that they have those controls". One participant here mentions the complacent attitude of platforms, describing them as "waking up too late".

Numerous participants also cite the hesitation of organizations to offer detailed insights into their internal processes as a significant challenge. This hesitancy largely stems from a desire not to "reveal what's under the bonnet or disclose their algorithms, etc.", fearing it might compromise their competitive edge. Such resistance to disclosing critical operational information underscores the difficulty of maintaining transparency while safeguarding strategic benefits.

Despite the above requirements, participants expect the EC to be lenient with VLOPS and the results of audits in the first year: "I don't expect VLOPS to be fined immediately, but rather that the EU will be interested in seeing, if VLOPS are not compliant, what actions they undertake to comply in the future."

In summary, the challenges around DSA audits in the first year highlight the pressure on VLOPS and auditors due to high assurance requirements and late guidance. According to interviewees, VLOPS therefore struggle to demonstrate compliance while also protecting their competitive advantage. Despite this, it is hoped that the EC will take an understanding approach aimed at future improvements. This situation again highlights the importance of cooperation between the EC, auditors, and platforms for more effective DSA compliance.

4) Decentralised nature of platforms and organisational oversight

The novelty of regulation is also seen as a challenge, participants noting that this is really the first time the technology sector, in this area, has been put under such scrutiny. "Online platforms have never been subjected to such an audit, unlike banks, which have whole compliance teams dealing with legislation and controls" one participant emphasizes. Another adds, "This is the first time they are being regulated in the online domain," and "the DSA really hits them at their core business."

On top of this, and this is highlighted by one participant as a "culture thing", tech companies often consist of individual engineering teams that have a lot of freedom. A participant mentions that in an organization they worked for, different teams work decentrally on their own expertise: "You have a team for podcasts, a team for playlists, a team for artist profiles, you have a team for search, these operate in a decentralised way and often don't know exactly what they do from each other either". The motto here is "move fast and break things" where the focus is on developing and rolling out new features, rather than documenting how and why this is done.

One interviewee points out the challenge of translating technical terms between different teams within an organisation and describes this as, "translating technical things, where you've got technical concepts on one side within the business, and then also, compliance itself can have quite a lot of technical concepts. So, it's just that kind of mutual understanding and translation piece." She also stresses the importance of internal communication between teams and interpreting complex concepts on both sides with: "it's that kind of internal communication between teams and interpreting complex kind of concepts on both sides." These comments highlight the importance of mutual understanding and effective communication in bridging the gap between technical and compliance-related aspects within organisations.

The novelty of the legislation and decentralised nature of organisations also make it difficult for companies to gain an overall perspective. "You see many companies don't have a holistic approach" and "getting a holistic and complete overview, they find that very difficult". Many online platforms have a good trust and safety department, which, for example, looks at content moderation and policies because as one describes it: "there has been pressure on that from a social point of view for years". But in other areas, such as being transparent about how Recommender Systems work, there has never been this pressure, as a participant stresses, "They often have no idea what kind of models they have across the breadth of their entire platform that can be legally classified as a recommender system".

A participant indicates that within the organisation she works for, it is a significant challenge to gather information from every segment and team in the company. She explains, "It's not just one team that does it, you need to draw on data are in each drawer on teams from across the business. So yes, it's very much needing a cross functional effort, which, which is a big piece of work." This highlights the need for a cross-disciplinary effort, where collaboration between different departments is essential to collect the required data and insights company-wide.

Another participant adds to this that getting a holistic view is a big problem and often involves thousands of applications: "At a VLOP we work for, they had over 1,000 applications of profiling techniques and Recommender Systems", raising the question of how to "roll this up into something that can be reported".

The introduction of the DSA marks a significant milestone by applying comprehensive regulation for the first time within the technology sector, an area that previously had little to no oversight. This represents a significant challenge for online platforms, which traditionally operate with decentralised engineering teams focused on rapid development without extensive documentation or compliance structures. Moreover, their decentralised nature and emphasis on innovation makes it difficult for them to gain a holistic overview and understanding of their operations, especially in areas such as recommender systems. This highlights the need for online platforms to rethink their approach to compliance and internal coordination and strive for a more structured and holistic approach to their business processes.

5) Resource scarcity and lack of expertise within online platforms

The DSA also brings challenges in terms of resources and expertise. "They definitely have the resources, especially the big platforms," one participant notes, yet internal expertise and willingness appear to be bottlenecks. Interpretations and approaches, here again, vary from company to company. It's mentioned in several interviews that it's a matter of risk assessment, with companies not wanting to overcommit to legislation, but also not wanting to do too little: "It's also a matter of waiting, reluctance, and compliance is, in this respect, about weighing your chances. Making a risk assessment of impact. So, what are the costs of non-compliance and what's the likelihood of getting caught?"

Another participant highlights the significant costs for online platforms to comply with such legislation: "if you look at a party I worked for, they had to hire hundreds of people to solidify that content moderation aspect, not to mention the fee they have to pay the EC for supervision, the staff they have to pay. It really amounts to hundreds of millions, I think."

Moreover, platforms often do not have the expertise needed internally to comply with the DSA. This requires a multidisciplinary team with people with IT audit, lawyers, strategists, developers, et cetera. as one participant emphasizes. "These platforms have resources, but not the right kind of resources. There are often many lawyers who are good at interpreting a certain legal text, but when it comes to

actually taking action and implementing and really thinking it through with a risk control perspective, that's where outside counsels or we as advisory firms come in."

Another participant highlights the lack of manpower at platforms: "You could say that at the moment and in the near future, they don't have enough people and also not enough people who understand this because a whole new reality is being created by this legislation."

In summary, this creates a complex balance between the availability of resources and the need for specialised expertise within online platforms. While major platforms have significant resources, the challenge lies mainly in internal expertise and willingness to comply with legislation. Companies weigh the risks and costs of non-compliance against the likelihood of enforcement, leading to varying degrees of engagement with the DSA. The significant costs associated with DSA compliance, e.g. content moderation, highlight the financial impact on platforms. Moreover, there is often a shortage of staff with the required multidisciplinary expertise, necessitating the use of external consultants. This lack of manpower and specialised knowledge poses significant challenges to compliance.

6) Difference in interpretations and sentiment of smaller platforms

The DSA is interpreted differently by online platforms, partly due to the lack of guidance from the EC. One notable aspect is how platforms approach their "terms & conditions"; some spread them across multiple pages to get out from under certain DSA obligations, while others centralise them. These differences in approach illustrate the variability in how the law is interpreted, with some platforms interpreting the law "to their own advantage."

Specifically, differences in approach to transparency reports are highlighted: "Some organisations really structurally choose to give as little detail as possible". Which goes against the intention of the DSA. The difference in the number of controls - ranging from "20 Controls" to "200 Controls" - further highlights the diversity in compliance strategies and interpretation of complying with items such as protection of minors or recommender systems. These differences in interpretation are compounded by the lack of uniform guidelines, leading to "every company doing it differently, with different depth, different scope." One participant adds: “that would be the case with a control-based audit anyway. Because, of course, there are different ways to demonstrate that you are in control and at different levels."

Among smaller platforms, there is a clear sentiment of doubt and reluctance towards the DSA. Many of these platforms adopt a wait-and-see attitude, driven by the perception that there is little chance of regulators actually intervening: "Well, nice that we have to do all this, but yes, no audit, so why should we?" This attitude is reinforced by the idea that "that regulator, it's going to be super busy, so well, I believe it when I see it. Why should we be compliant?" Nevertheless, some recognise that non-compliance carries risks, especially when it comes to the need to respond quickly to requests without proper documentation: "If you don't have it written down then, you're not going to be able to respond to it within two weeks."

Despite this mostly laconic attitude, there are also platforms "that are close to being a VLOP" and proactively requesting gap analyses, recognising that "doing nothing at all is really not an option". This suggests that there is an awareness within the sector of the need for compliance, although the urgency and capacity to meet the requirements vary. Smaller platforms feel the urgency less and also have less capacity to comply with the DSA.

All this suggests that there are significant differences in interpretation and compliance strategies among online platforms, partly due to a lack of clear guidance from the EC. This variability manifests itself in the approach to "terms & conditions" and e.g., transparency reports, with platforms varying

in the level of detail and number of controls implemented, which in turn indicates varying approaches to compliance and interpretation of the law. Among smaller platforms, there is a mixture of reluctance and slow acceptance of the need for compliance with the DSA. While some postpone or defer the requirements of the DSA, others begin to acknowledge the reality of the new regulation and take steps to meet the requirements, despite limitations in budget and capacity.

7) Content moderation

Another challenge that online platforms struggle with is content moderation and its organisation, with regional differences and the balance between freedom of expression and the removal of illegal content being key.

The DSA requires platforms to take proactive measures to detect and remove illegal content. This presents platforms with the dilemma of how strict moderation should be applied without undermining freedom of expression. A platform has the choice to emphasize content moderation or freedom of expression, as indicated by a participant's remark: “I do know that, for a company we work for, they still have some freedom to emphasize either content moderation or freedom of expression.” The participant emphasizes that it's often a strategic choice and mentions Twitter/X as an example, where a strategic choice is made for freedom of expression. Mistakes in this balancing act can lead to legal sanctions, but also to public backlash if users feel that their rights are being restricted.

The complexity of content moderation is also highlighted, especially for companies dealing with user-generated content (UGC). UGC poses significant challenges due to the vast diversity and volume of content produced and shared by users on online platforms daily. Firstly, the amount is overwhelming, making effective monitoring and moderation a logistical and technological challenge. The enormous volume of uploads per day makes it impossible to review all content manually. This requires advanced automation techniques, which are still in development and cannot always accurately identify illegal or harmful content. As emphasized by a participant: “Those algorithms can, in most cases, recognize a weapon, or a bomb. But yeah, recognizing that Mark Rutte says something wrong with AI modified. That is, of course, almost impossible.”

There is also enormous variability in user-generated content in terms of content, context, and intention, for example. And this makes uniform moderation rules difficult to apply. What is considered harmful in one context may be completely innocuous in another. This requires some understanding of cultural, social, and political nuances that are difficult to fully automate. The remark about the difference between companies like Booking, which mainly deal with structured data and no UGC, underscores how the nature of the content affects the complexity of content moderation. For companies without UGC, compliance with the DSA is considerably less complex since they do not have to worry about the constant flow of new, unfiltered user content.

In essence, the presence of UGC makes content moderation one of the most challenging aspects of DSA compliance. It requires a careful balance between protecting users from illegal and harmful content and maintaining their right to freedom of expression while navigating technological, legal and operational constraints.

8) New systems and functionalities

Another topic mentioned in multiple interviews is the need to develop new systems or adjust existing ones due to the requirements of the DSA. Examples of this can be seen in reporting content and content moderation. It particularly emerges that, to date, due to the low volume, at some platforms, very simple systems suffice, involving many manual steps. However, with new requirements, the volume increases, raising the question of whether platforms can handle this. As one participant

emphasizes: “I've seen it at a platform, where I wonder if they can keep up, so yes, then you really will have to build something else, but they can do it. It just again costs resources, which are scarce.”

In addition, a participant points out that certain DSA articles require significantly more technical effort than others. She explains this with the example: "things like the non-personalised alternatives for recommender systems, you know, that's something that obviously had to be created as a whole new product."

Several interviews reveal that, in practice, platforms take two different approaches to content moderation. On one hand, there are companies that use existing content reporting systems, designed for community guidelines, and add a new workflow to them. On the other hand, there are companies that take an integrated approach without developing new functionalities. One interviewee mentions that within her organisation, content moderation is mainly built upon existing systems: "So I think a really big thing has been looking at what we can build upon and leverage existing systems, we build upon it to make sure that we have something that fits all the requirements."

These statements point to the need for online platforms not only to adapt their technical infrastructure, but also to overhaul their operational and organisational structures. This is essential to meet the increased requirements of content moderation, transparency and accountability imposed by the DSA. Here, the transition to automated systems seems inevitable, given the scale and complexity of the challenges ahead.

9) Multiple Regulations Worldwide

A recurring theme in several interviews is the challenge that online platforms face when navigating through the complex landscape of multiple regulations. Highlighting the importance of a well-developed compliance team, equipped to deal with various future regulations in this sector, strongly emerges. One interviewee explains, "The problem for the platforms is that the DSA is one of many and they really need to get used to a higher level of supervision and they need to start designing their organisation accordingly." This illustrates the need for platforms to adapt their structures to an increased level of regulation.

Furthermore, the current capacity issue is highlighted by another interviewee, who states, "I think there is also really a lot coming at them now and they cannot cope with that in terms of capacity." This is reinforced by another interviewee: "You really need a more mature compliance apparatus for that. A lot of platforms don't have that," indicating a general lack of preparation within the industry.

The consensus among several interviewees is clear on the need for online platforms to develop a compliance team or programme suitable for complying with multiple future regulations: "You want to set it up in such a way that it's fit for use for the DSA, but also for the Online Safety Act, DMA, AI Act, and other upcoming legislations, so that implementation becomes increasingly less time-consuming." Another emphasizes the following: "You want to reuse the same people, the same processes, the same controls, to comply with all those legislations."

In conclusion, these insights underline the importance for online platforms to develop robust, multi-faceted compliance strategies. It is not just about complying with current regulations such as the DSA, but also being prepared for future legislations. This requires significant investments in both human and physical resources to build a compliance team or infrastructure capable of handling the complex requirements of multiple regulations.

10) Challenges for the EU and the importance of enforcement and supervision

In various interviews, there is an expectation that the Digital Services Act (DSA) will become the new global standard for regulating online platforms. One of the interviewees clearly states: "Yes, I think this will become the standard. Look, Europe is just very progressive with legislation on data and digitalization, and the DSA is one of those." This statement underscores Europe's leading role in digital legislation and the potential of the DSA as a guiding framework.

In addition, the concept of the "Brussels effect" is mentioned several times, with the influence of European regulations extending globally. Several interviewees here mention the UK's Online Safety Act, which shows overlapping elements with the DSA. Another interviewee mentions that the rest of the world “tends to follow," indicating the potential of the DSA to influence international norms.

However, the universality of the DSA is tempered by some interviewees' comments on the dependency on the response from the United States. The influence of American legislation is seen as crucial for the DSA to become a standard. "If they enact legislation in this direction, then absolutely a standard, if they leave it as it is, then not really, because you already see that platforms just have two different apps in different parts of the world."

An interviewee says: “I think particularly on these topics awareness is important.” Another makes the comparison with the GDPR, emphasizing the importance of awareness: “And the GDPR, yes, although it is certainly not the holy grail of privacy legislation, it has achieved a goal of the GDPR, and that is awareness that people have become more aware of what they are doing with personal data. And I think that is also a goal of the DSA that should not be underestimated.” This underscores that, besides regulating online platforms, a significant goal of the DSA is to create broader awareness of the impact of digital services on society.

Multiple experts state that enforcement and supervision will be decisive for the success of the DSA. As one interviewee puts it: “Supervision will determine everything.” Another interviewee refers to GDPR supervision, mentioning that only a few specific elements of the law are supervised, leaving out elements like automated decision-making and transparency over profiling. The interviewee emphasizes: “You will see that with the DSA, 100%.” Another interviewee mentions that the Digital Service Coordinator (DSC) from Ireland indicated that for the first year, they have 3 or 4 focus areas, namely protection of minors, disinformation, and hate speech. This DSC explicitly states what the focus areas will be, but the interviewee stresses: “I don’t know how other countries, including the Netherlands, will handle this.” This shows that some regulators are already setting priorities for their enforcement efforts and highlights the importance of structured and uniform enforcement mechanisms to achieve the DSA’s objectives.

This supervision could become a problem, many experts mention the lack of manpower and expertise at both the European Commission and local supervisors, the DSCs. This is emphasized by several interviewees, "I think firstly capacity in general I think” and "Yes, I think manpower. That's really a very big challenge". Here, several experts also mention the number of vacancies open at the EC for the DSA enforcement team. "You can see that there are now a huge number of vacancies open at the European Commission." Another interviewee draws a parallel with the GDPR, emphasizing: “The Dutch Data Protection Authority is already chronically understaffed and facing problems.” These quotes point to a significant shortage of personnel equipped to carry out the complex and demanding tasks brought by the DSA. Without adequate manpower and knowledge, the effective implementation and enforcement of the DSA, and by extension any form of digital regulation, will be severely hindered.

4.3 Comparison of Results with Theory

The insights derived from the interviews add significant, practical depth to our understanding of the challenges faced by companies when complying with the DSA, offering real-world perspectives that are not as prominently discussed in the literature. These insights provide a nuanced view of the operational realities, strategic considerations, and compliance strategies employed by online platforms, which can enhance our understanding of the practical implications of DSA compliance.

In the theory, the legal complexity of dealing with multiple regulations, including the GDPR, DMA, and AIA, is discussed by Đurović & Kniepkamp (2022), Greif & Grosz (2023), Hacker (2021), Morozovaite (2023), and Rudohradská & Trescáková (2021). Additionally, the lack of clear guidelines on influencer marketing and parody content is highlighted by some, including Duivenvoorde & Goanta (2023) and Pakutinskas & Šepetys (2023).

The complexity of managing multiple regulations is emphasized by several experts. Online platforms face the challenge of navigating a complex regulatory landscape, necessitating the development of advanced compliance structures to meet future regulations. Various interviewees highlighted current capacity issues and pointed out the need for a mature compliance apparatus that many platforms currently lack to effectively handle the onslaught of new regulations. The consensus underscores the importance of establishing robust compliance teams or programs that are adaptable not only for the DSA but also for upcoming legislation such as the Online Safety Act, DMA, AI Act, and others, thus enabling a more efficient and less time-consuming implementation.

Furthermore, the absence of clear guidelines is confirmed and elaborated upon as the greatest challenge by all experts. Interviews reveal that the openness to interpretation, the numerous ambiguities, and vague terms, and the lack of guidance are among the greatest frustrations for online platforms and those who have to work with them. Experts also emphasize that this leaves considerable room for online platforms to interpret these in their own, likely advantageous, ways. This issue is further illuminated by the differing perspectives between lawyers who write the laws, companies that must comply, and auditors who test them.

Moreover, there is a lack of audit standards and an industry standard. The delegated act for auditors has been issued but shows ambiguities, inconsistencies, and is incomplete—likely due to the involvement and subsequent absence of IT audit experts in its drafting. Participants emphasized significant differences in transparency reports, risk management matrices, and system risk assessments among companies. There is consensus on the need for more uniform control standards to ensure the reliability of control advice. Despite ongoing discussions among stakeholders, including the Big Four, to establish a uniform audit framework compatible with ISAE 3000, the European Commission has not yet adopted proposed standards. This situation has led to uncertainty for both auditors and online platforms about the future of DSA audits, highlighting the urgent need for standardized procedures and clearer guidelines to enhance the effectiveness and consistency of these audits.

The requirement for VLOPS to undergo rigorous audits for reasonable assurance and operational effectiveness in the first year of DSA enforcement is seen as particularly demanding. These audits also cover a period rather than just a moment in time. The late issuance of additional audit guidelines, combined with high assurance demands, leads participants to anticipate predominantly negative audit results. Many VLOPS say they struggle with time constraints and lack sufficient evidence of their control processes, and some hesitate to disclose detailed internal activities to protect their competitive advantages. Despite these challenges, there is an expectation that the European Commission will be lenient in the first year regarding VLOPS, focusing more on future compliance efforts than on

immediate penalties. This situation underscores the need for effective collaboration between the EC, auditors, and platforms to improve DSA compliance.

Content moderation is another topic that arises from the theory, with Bayer (2022), Mazúr & Gramblička (2023), Farrand (2023), Kucina & Univ Latvia (2022), Mezei & Szentgáli-Tóth (2023), and Reviglio & Santoni (2023) addressing the complexity of balancing content moderation and freedom of expression. They also note that the interpretation of what is illegal or harmful is subjective and varies by country. From discussions with experts, it is clear that online platforms indeed struggle with this, and a platform can emphasize content moderation or freedom of expression itself. What is not highlighted in the theory but comes out in the interviews is primarily the operational challenge behind content moderation. Here, companies dealing with user-generated content (UGC) face difficulties in handling a significant increase in volume, making this a logistical and technological challenge. Additionally, the variability of UGC poses another challenge, where the context and intention of content make it difficult to apply uniform moderation rules.

In the literature on the DSA, operational and resource challenges are not extensively discussed. Đurović & Kniepkamp (2022) state that compliance with the DSA requires new solutions, not just system adjustments, but a complete overhaul or new system building. An example of such a system, namely an Alternative Dispute Resolution (ADR), is highlighted by Greif & Grosz (2023), who note that such a system requires a significant investment and many resources.

Experts validate these challenges and note that, for example, reporting and moderating content indeed requires new systems and functionalities. Interviews also show that, to date, due to the low volume, very simple systems suffice for various platforms, but whether these can withstand the expected increase in volume is in question. It also appears that platforms take different approaches in creating systems and functionalities; some build on top of existing systems and see how they can leverage these systems, while others create new systems entirely.

Another challenge that is less mentioned in the theory but emphasized by experts is resource scarcity and the lack of expertise within online platforms. By the way, it is mentioned multiple times that large platforms have the resources, but it is about a risk assessment, where platforms do not want to do too little, but especially not too much. For instance, a participant estimated amounts in the hundreds of millions for larger platforms. Due to the scale of the legislation, it is difficult to find qualified personnel, and online platforms often have enough lawyers but lack people who think from a risk control perspective, which is where outside counsels or advisory firms can play a role.

Another operational challenge not mentioned in the theory but arising from the interviews is the decentralized nature of platforms and the difficulty they have in obtaining an organizational overview. It is also noted that this is the first time that online platforms are really being regulated, and unlike, for example, banks, they have no or no extensive compliance teams.

Additionally, it is highlighted that platforms and tech companies generally consist of individual engineering teams that work independently and with a lot of freedom on their functions and projects. Here, the challenge of translating technical terms between different teams is mentioned, emphasizing the importance of mutual understanding and effective communication in bridging the gap between technical and compliance-related aspects. Especially since, for example, transparency reports require information from every corner of the organization, making cross-functional effort necessary.

It also appears that platforms, due to social pressure in recent years, have a good trust and safety department that focuses on content moderation, but this focus on other areas, such as transparency around how recommender systems work, is not present, and platforms often do not know which functions they have across the organization that can legally be classified as recommender systems.

Challenges around data privacy and whether the DSA goes far enough to counter algorithmic manipulation, as expressed in the literature by Hacker (2021), are not validated by interviewees. Several people mention that the DSA is a step in the right direction, and that it initially involves awareness, as was also the case with the GDPR. And it makes sense to start with the largest platforms.

The challenge of technological evolution and its impact, mentioned by Morozovaite (2023), is still validated and emphasized as a fact that applies to both sides of the spectrum, for both online platforms and the EC and policymakers. Evolving business models may require continuous adaptation to stay compliant with evolving regulations, and this also works the other way around.

Another finding, although not really a challenge for platforms themselves, is that the DSA is interpreted differently by online platforms, largely due to vague guidelines from the EC. This leads to different strategies in managing, for example, general terms and conditions and transparency reports, where some platforms minimize details to evade DSA obligations, while others use compliance as a competitive advantage. Among smaller platforms, there is a wait-and-see attitude, driven by skepticism about the enforcement of the regulation, although some larger platforms are beginning to recognize the risks of non-compliance. It can thus be said that there are many different approaches and interpretations among platforms, influenced by the lack of clear guidelines from the EC and the different capabilities to meet this new regulation.

Challenges for the EC and policymakers are also mentioned in the literature. While Dumancic (2021) and Nóra Kiss (2023) both emphasize the need for harmonization of digital laws across the EU, and state that this is a complex process that requires a careful balance between the powers of countries and the EU. Dumancic (2021) and Huckova & Semanova (2022) highlight the challenge of balancing regulation and innovation for the EU and its policymakers is significant, as it directly impacts the region's ability to remain competitive and innovative in the global digital economy. They state balancing this requires a nuanced approach to ensure regulations such as the DSA protect users and promote fair competition. In the interviews, it is emphasized that the success of the DSA fully depends on the capability of the EC and DSCs to enforce successfully. Unlike the literature, the interviews primarily mention practical challenges for the EC and enforcers, such as the lack of capacity and skilled people, and it is also emphasized that there are already chronic understaffing problems at these institutions.

The interviews conducted provide insights of great value that enrich the theoretical discussions surrounding the DSA. They add detailed perspectives on the operational challenges of content moderation, the complicated dynamics of compliance systems within online platforms, and the practical issues of audit processes. Furthermore, they shed light on the decentralized nature of platform operations and the nuances of inter-team communication, which are less discussed in the existing literature. These discussions not only fill gaps in the literature, but also underline the complexity of implementing these regulations in real-world scenarios.

4.4 Risk Mitigation Framework

In this section, we present the results of the interviews and develop a risk mitigation framework. This framework, designed to address the challenges faced by online platforms, is constructed around the themes that emerged during the interviews. It integrates insights primarily derived from these

interviews, supplemented by existing literature that serves as the foundation for the collected empirical data.

The framework systematically identifies potential pitfalls, ranging from the ambiguity in regulatory texts and inconsistent application across platforms, to the complexity of content moderation and the integration of new systems and functionalities. For each identified challenge, the framework outlines the corresponding risks and proposes a series of mitigation measures. These measures range from seeking expert legal advice, proactive engagement with regulators and developing internal compliance frameworks, to leveraging advanced content moderation technologies and investing in scalable systems.

This strategic approach aims to guide online platforms in enhancing their compliance position, thereby minimizing the risk of non-compliance and improving operational efficiency. The risk mitigation framework, primarily built from stakeholder practical experiences and enriched with scholarly insights, offers a comprehensive strategy to navigate through the complexity of DSA compliance.

The risk mitigation framework is shown below in Table 10, after which it will be discussed in detail in section 4.5.

Table 10 Risk Mitigation Framework for Online Platforms

Challenges	Meaning for online platforms	Risks	Risk mitigation measures
Openness to interpretation and lack of guidance	Struggle with vague terms and the absence of clear guidelines, leading to compliance uncertainty.	Misinterpretation leading to non-compliance	**1. Seek expert consultation and legal advice:** Engage with legal experts specializing in digital law to gain clarity on compliance obligations. **2. Proactive engagement with regulators:** Communicate with regulators to seek clarifications and advocate for clearer guidance. **3. Develop internal compliance frameworks:** Create standardized processes and training to ensure consistent application of vague and ambiguous terms across the organization. **4. Continuous monitoring and adaptive compliance strategies:** Establish processes for ongoing regulatory monitoring and adapt compliance strategies as more guidance becomes available. **5. Centralized compliance leadership:** Set up a centralized body responsible for interpreting regulatory requirements and ensuring strategic alignment across the organization.
		Inconsistent application across the platform	**1. Regular compliance training:** Implement comprehensive training programs for employees to ensure a unified understanding of compliance requirements across different departments. **2. Internal audits:** Conduct regular internal audits and reviews to identify and rectify inconsistencies in the application of compliance standards.
		Interpretation at odds with EU expectations (e.g., protection of minors)	**1. Best practices and benchmarking:** Research and implement industry best practices for ambiguous areas like the protection of minors, and benchmark against peers. **2. Risk assessments and scenario analysis:** Conduct risk assessments and scenario analyses to better understand how different interpretations may or may not align with EU expectations and adjust practices accordingly. **3. Stakeholder engagement:** Engage with stakeholders, including child protection organizations and experts, to gain insights into best practices for protecting minors in line with EU expectations.
		Strategic misalignment and misallocation of resources	**1. Compliance and business strategy sessions:** Ensure that compliance strategies are integrated into the broader business strategy to prevent misalignment. **2. Resource allocation reviews:** Regularly review resource allocations to compliance efforts to ensure they are proportionate and effective.
Lack of audit standards	Variability in audit practices due to lack of standardised frameworks, making it hard to	Inconsistencies in compliance assessments	**1. Collaborative industry efforts:** Engage in or initiate industry-wide efforts to develop shared auditing frameworks for DSA compliance. Participation in working groups or other of that nature aimed at addressing these standards can help in creating a more uniform approach. **2. Leverage external expertise:** Until standardized frameworks are established, platforms can engage with external auditors who have experience in similar regulatory audits to ensure that their practices align with the highest industry standards.

	ensure consistent compliance.	Lack of clarity on audit expectations	**1. Active dialogue with regulators:** Establish a continuous dialogue with the European Commission and other regulatory bodies to gain clarity on audit expectations and to advocate for the development of specific audit standards for the DSA. **2. Documentation and transparency:** Maintain comprehensive documentation of audit processes, decisions, and interpretations of the DSA. This transparency can support platforms in case of regulatory scrutiny and demonstrate a good faith effort towards compliance.
		Insufficient audit readiness	**1. Internal training and awareness:** Implement training programs for staff on what to expect from audits and how to ensure that their operations are prepared for scrutiny, improving overall audit readiness. **2. Peer reviews and benchmarking:** Participate in peer reviews and benchmarking exercises with similar platforms to understand best practices in audit preparation and execution, as well as in compliance practices, enhancing the overall quality of audits received.
Audit reports and time constraints	Pressure from high assurance requirements and late guidance, making it challenging to demonstrate compliance.	Inability to meet high assurance requirements	**1. Early preparation and evidence gathering:** Start the audit preparation process early, even before the guidance is published. Implement a continuous audit readiness program to collect and maintain audit evidence throughout the year.
		Regulatory penalties and fines for non-compliance.	**1. Regulatory engagement and e.g., remediation plans:** Maintain proactive communication with regulators, demonstrate compliance efforts, and negotiate penalties while presenting remediation plans.
Decentralised nature and organisational oversight	Difficulty in gaining a holistic understanding of operations due to decentralized structures and rapid development cycles.	Lack of compliance due to isolated information and lack of coordination between different departments.	**1. Central compliance function:** Establish a central compliance or coordination team responsible for overseeing and integrating compliance efforts across various departments and teams.
		Difficulty in translating technical and compliance concepts across teams.	**1. Cross-functional teams:** Form cross-functional teams that include e.g., IT experts, lawyers, strategists, and developers to ensure a unified approach to development and compliance. **2. Training and knowledge sharing:** Provide regular training sessions and workshops for employees to foster mutual understanding of technical and compliance issues, enhancing internal communication.
		Inability to provide a holistic overview of operations, (e.g., in complex areas like recommender systems.)	**1. Holistic operational review processes:** Implement regular review processes that require input from all departments to gain a comprehensive overview of operations, focusing on areas like transparency in recommender systems. **2. Documentation and process standardization:** Implement standardized documentation practices and processes for all teams, emphasizing the importance of compliance alongside innovation.

Resource scarcity and lack of expertise	Challenges in aligning resources and expertise with the requirements of the DSA, affecting compliance efforts.	Inadequate internal expertise leading to potential non-compliance.	**1. Training and development:** Invest in specialized training programs to upskill existing staff in critical areas such as IT audit, legal compliance, and risk management. **2. Hiring and outsourcing:** Invest in hiring new staff with the required expertise and consider outsourcing certain compliance tasks to external service providers to mitigate manpower shortages.
		Reluctance and waiting strategy risking late or insufficient compliance efforts.	**1. Strategic risk assessments:** Implement strategic risk assessment frameworks to better understand the costs and implications of non-compliance versus the investments needed for compliance, which helps with e.g., informed decision-making.
		Lack of multidisciplinary expertise and manpower to meet diverse compliance requirements.	**1. Cross-functional compliance teams:** Form cross-functional teams that include IT experts, lawyers, strategists, and developers to address the multidisciplinary nature of compliance challenges. **2. Hiring and outsourcing:** Invest in hiring new staff with the required expertise and consider outsourcing certain compliance tasks to external service providers to mitigate manpower shortages. **3. Partnerships with advisory firms:** Establish strategic partnerships with external advisory firms to access specialized expertise, when necessary, but also focus on building internal capabilities over time to reduce dependence.
		High costs of compliance straining financial resources.	**1. Efficient resource allocation:** Plan and allocate resources in a certain way to prioritize compliance efforts that offer the most significant impact, considering both the costs of compliance and the penalties for non-compliance.
Content moderation	Balancing freedom of expression with the need to remove illegal content, while dealing with the volume and complexity of UGC.	Over-moderation leading to suppression of freedom of expression.	**1. Clear content guidelines and user education:** Develop and communicate clear content guidelines to users, emphasizing the balance between freedom of expression and the need to remove illegal content. Engage in user education campaigns to foster a better understanding of content policies.
		Under-moderation leading to the spread of illegal or harmful content.	**1. Advanced detection technology:** Invest in and continually improve advanced content detection technologies so illegal or harmful content can more accurately identified, while minimizing false positives. Here an example could be to train certain machine learning algorithms with diverse datasets to enhance accuracy.
		Legal sanctions or public backlash due to failure in balancing content moderation efforts.	**1. Ongoing dialogue with stakeholders:** Maintain an ongoing dialogue with regulators, civil society, and users to understand concerns and expectations around content moderation. Use feedback to refine moderation policies and practices.
		Technological challenges in accurately identifying complex content	**1. Human-in-the-loop processes:** Implement a human approach for content moderation, where automated systems flag content for review, and trained human moderators make the final decision, especially in complex cases involving cultural, social, or political nuances.
		Difficulty in applying uniform moderation rules due to variability in UGC.	**1. Contextual moderation policies:** Develop moderation policies that are flexible enough to account for the variability in content, context, and intention. This may include setting up specialized moderation teams for different types of content or regions, who are knowledgeable about the specific cultural, social, and political contexts.

		Operational constraints in managing the volume of UGC.	**1. Scalable moderation strategies:** Adopt scalable content moderation strategies that can adjust to the volume of UGC, such as tiered review systems where content is prioritized based on potential risk or impact. Invest in capacity building to ensure that content moderation efforts can scale up as needed.
New systems and functionalities	The need to develop or adjust systems to meet DSA requirements, often requiring significant resource investment.	Inability to handle increased volume of content moderation and reporting due to inadequate systems.	**1. Scalable system development:** Focus on developing scalable systems that can handle increasing volumes efficiently. This includes investing in automation and machine learning technologies for content moderation and reporting functionalities.
		Resource scarcity impacting the development or adjustment of new systems.	**1. Resource allocation and planning:** Prioritize resource allocation towards the development and enhancement of critical systems. This may involve reallocating budgets to support technological upgrades.
		Difficulty in integrating new functionalities with existing systems.	**1. Integration frameworks:** Develop and utilize frameworks that facilitate the addition of new functionalities into existing systems. This could for example involve middleware solutions that allow for flexible integration while minimizing the need for extensive modifications to current systems.
		Overlooking the need for operational and organisational adjustments alongside technical upgrades	**1. Holistic approach to system development:** Ensure that the development or adjustment of systems is accompanied by corresponding operational and organisational changes. This could involve training staff on new systems, adjusting workflows to accommodate new functionalities, and fostering a culture of continuous improvement and adaptation to change.
Multiple regulations worldwide	Navigating through a complex landscape of various regulations, necessitating robust compliance teams.	Overwhelmed by the complexity and volume of regulations.	**1. Unified compliance framework:** Develop a unified compliance framework that can adapt to multiple regulations. This includes creating standardized processes that can be applied across different legal requirements to streamline compliance efforts.
		Inefficient use of resources due to managing compliance in isolation.	**1. Centralized compliance management system:** Implement a centralized compliance management system that allows for the tracking, management, and reporting of compliance activities across all regulations, enhancing efficiency and reducing redundancy. **2. Investment in compliance talent and technology:** Invest significantly in both compliance talent and technology to build a compliance infrastructure capable of handling complex requirements.
		Lack of preparedness for future regulations.	**1. Future-proof compliance planning:** Engage in continuous legal and regulatory monitoring to anticipate future changes and adjust compliance strategies accordingly. Examples here could be scenario planning and investment in flexible technology solutions that can adapt to new requirements.
		Difficulty in maintaining compliance consistency across regions.	**1. Regional compliance teams:** Establish regional compliance teams that understand local regulations and can ensure that global compliance strategies are effectively implemented at the local level. This helps in addressing regional variations in laws and regulations.

4.5 Discussion of Risks and Mitigation Measures

In this paragraph, we shortly discuss the risk mitigation measures that emerge from the framework.

Openness to interpretation and lack of guidance

Interviewees highlighted the DSA's openness to interpretation and lack of clear guidelines as key challenges, which added uncertainty to compliance efforts. This has been exacerbated by the use of ambiguous and vague terms within the DSA, which online platforms must interpret independently. The risk mitigation framework proposes several measures to address these issues, including seeking expert advice, proactive engagement with regulators, developing internal compliance frameworks, ongoing monitoring and establishing centralized compliance leadership. These strategies aim to reduce the risks of misinterpretation and non-compliance by promoting clarity and consistency in the interpretation of the provisions of the DSA.

Lack of audit standards

The variability in audit practices due to the lack of standardized frameworks emerged as a concern, making it difficult to ensure consistent compliance. The framework recommends joint industry efforts to develop shared audit frameworks, leverage external expertise and maintain an active dialogue with regulators. These measures can help create uniformity in audit practices and clarity on audit expectations, improving the overall quality of DSA compliance reviews.

Audit reports and time constraints

The pressure of high assurance requirements and late guidance creates challenges in demonstrating compliance. To mitigate these risks, the framework recommends early preparation and evidence gathering, as well as a commitment from the regulator to demonstrate compliance efforts and negotiate penalties while remediation plans are presented. These steps can help platforms meet the DSA's strict audit requirements despite time constraints.

Decentralised nature of platforms and organisational oversight

The decentralized structure of many online platforms makes achieving a holistic understanding of business operations difficult, a key challenge highlighted by interviewees. The risk mitigation framework emphasizes the establishment of a central compliance function, the formation of cross-functional teams and the implementation of holistic operational review processes. These measures can facilitate better coordination and integration of compliance efforts across different departments and teams.

Resource scarcity and lack of expertise

Interviewees noted the difficulty in matching resources and expertise to the requirements of the DSA. To address this, the framework proposes investing in training and development, hiring and outsourcing staff, forming cross-functional compliance teams and building partnerships with consulting firms. These strategies are aimed at strengthening the internal expertise and manpower needed to effectively navigate the DSA compliance landscape.

Content moderation

Content moderation poses a significant challenge, especially when balancing freedom of expression and the need to remove illegal content. The framework recommends clear content guidelines, investments in advanced sensing technology, ongoing dialogue with stakeholders and implementation of human-in-the-loop processes. These measures are intended to increase the accuracy and fairness of content moderation efforts.

New systems and functionalities

The need for new or updated systems to meet DSA requirements emerged as a theme that required significant investment in resources. Scalable system development, resource allocation and planning, and integration frameworks are among the proposed mitigation measures. These strategies focus on developing technological and operational capabilities to meet the requirements of the DSA.

Multiple regulations worldwide

Navigating the complex landscape of multiple regulations was seen as a challenge, requiring robust compliance teams. The framework proposes the development of a unified compliance framework, investments in compliance talent and technology, and the creation of regional compliance teams. These measures are intended to streamline compliance efforts and ensure consistency across regulatory environments.

4.6 Conclusion of Results

The conclusion of this chapter, which reflects on the challenges of DSA compliance and the resulting risk mitigation framework, captures the essence of the regulatory landscape facing online platforms. This analysis, based on both literature and empirical data, underlines the urgent need for online platforms to refine their compliance strategies to deal with the complexities introduced by the DSA.

The DSA presents a wide range of challenges, ranging from the ambiguity of the text to the decentralized structure typical of technology companies. Its openness to interpretation and lack of clear guidance create significant uncertainty, which not only hinders compliance efforts difficult, but also threatens the effectiveness of the DSA itself. This is exacerbated by the lack of standardized audit frameworks, which leads to variability in compliance assessments, further diluting the consistency and reliability of such efforts.

Furthermore, the empirical evidence from the interviews highlights the operational and strategic adjustments required within platform structures to effectively address these regulatory challenges. The diversity in the stance of platforms, from those proactively adapting to those taking a wait-and-see approach, reflects the wider industry uncertainty about how best to meet the DSA's demands. This is especially true for smaller platforms, which may not have the resources and expertise to fully meet the requirements.

The risk mitigation framework developed in this chapter serves as a blueprint for online platforms. It advocates a more structured approach to compliance, emphasizing the need for clear internal guidelines, consistent application of DSA standards and proactive engagement with regulators. Furthermore, it underlines the importance of developing good internal compliance infrastructures that can adapt not only to the DSA, but also to future regulations that will affect the sector.

The discussions surrounding content moderation, the need for new systems and functionalities, and navigating multiple regulations worldwide illustrate the multifaceted challenges platforms face. These challenges require not only technological and operational adjustments, but also a cultural shift within organizations toward more integrated and transparent compliance practices.

In conclusion, as the DSA aims to set a global standard for the regulation of online platforms, the success of this legislative effort will depend heavily on the clarity of its guidelines and the effectiveness of its enforcement. Collaboration between regulators, platforms and other stakeholders will be crucial. Platforms must not only adapt to the immediate requirements of the DSA, but also anticipate future regulatory developments. This will require deeply integrating compliance into their strategic and operational frameworks. Platforms that successfully navigate these challenges can do more than just

ensure their survival; they will be well-positioned to flourish in an increasingly regulated digital landscape.

5 Discussion

This chapter explores the complicated dynamics between three critical stakeholders in the DSA compliance ecosystem: online platforms, the European Commission (EC) and regulators, and auditors. By integrating insights from interviews and the risk mitigation framework presented, we aim to clarify the specific challenges each stakeholder faces, discuss their current situation, and outline future steps to promote a more cohesive and effective compliance landscape. Additionally, this chapter compares results with theory, reflects on the broader implications of challenges, acknowledges the research's limitations, and suggests directions for future investigations, aiming for a cohesive approach to enhancing digital service regulation and compliance.

5.1 Interpretation of Results

Online platforms

Online platforms are struggling with the DSA's openness to interpretation and the resulting uncertainty around compliance. The lack of concrete guidelines and clear audit standards compounds these challenges, leaving platforms to follow a foggy compliance path filled with potential risks and strategic misalignments. Furthermore, the decentralized nature of many platforms increases the difficulty in achieving comprehensive oversight of operations, especially in areas such as content moderation and the implementation of new systems or functionalities to meet DSA requirements.

To address these challenges, platforms can increase their engagement with regulators, seek clarification, and advocate for more explicit guidance. Investing in internal compliance frameworks and staff training, as suggested by the framework, can increase the understanding and consistent application of the DSA across departments. Additionally, platforms must prioritize the development of scalable systems and processes that meet DSA requirements while maintaining operational efficiency. These are the main steps that online platforms can take, further steps are likely to follow after the audit assessment, and these steps will be highly dependent on the extent to which the EU aims to enforce the first years after introduction of the DSA.

European Commission (EC) and regulatory authorities

The EC faces the dual challenge of defining and disseminating clear, actionable guidelines for DSA compliance and establishing standardized audit frameworks. The variability in compliance assessments and the lack of uniformity in audits underscore the need for more definitive audit standards that address the DSA's unique requirements.

Improvements and future steps: The EC and regulators could focus on developing and sharing detailed, practical guidelines for implementing DSA, using insights from ongoing dialogues with platforms and auditors. Initiating joint efforts to establish shared audit frameworks could also help reduce inconsistencies in compliance assessments. Moreover, addressing the shortages of manpower and expertise within regulators is crucial for effective enforcement and supervision.

Auditors

Auditors are navigating a landscape characterized by a lack of standardized audit frameworks and clear expectations for DSA audits. The variability in audit practices not only poses a challenge to the consistency of compliance assessments, but also hinders auditors' ability to effectively measure platforms' DSA compliance.

To overcome these obstacles, auditors could benefit from industry-wide efforts to develop shared auditing standards, potentially aligned with existing frameworks such as ISAE 3000, where applicable. Strengthening the dialogue with the EC and the platforms can also provide clarity on audit expectations

and facilitate the development of audit standards. Peer reviews and benchmarking exercises can further improve audit quality and platform readiness.

5.2 Comparison with Theory

In this section, we will briefly compare the results of this study with the existing literature. For a more detailed comparison with theory, please refer to section 4.3, this placement was chosen to see what the differences were between theory and practice before the creation of the risk mitigation framework.

The general challenges arising from the literature on GDPR compliance are well documented and include ambiguities in requirements, limited resources, lack of clear guidelines and difficulty in understanding internal processes. These problems highlight significant obstacles to achieving compliance and underscore the need for unambiguous regulations, adequate resources and deep organisational understanding and training.

The suggestion that online platforms may face similar challenges under the DSA appears justified in retrospect. From the mostly predictive literature regarding the DSA, we can see that the legal complexity and, in addition, dealing with multiple regulations, including the GDPR, DMA, and AI Act, may become challenges. In addition, the literature by Duivenvoorde & Goanta (2023) and Pakutinskan & Šepetys (2023) gives a first indication on the lack of clear guidelines in the DSA. The literature also discusses the complex balance between content moderation and freedom of expression by several sources, including Bayer (2022), Mazúr & Gambličková (2023), Farrand (2023), and Kucina & Univ Latvia (2022). Moreover, literature recognises the need for online platforms to constantly adapt their business models to evolving regulations.

This research reveals that actual operational realities and strategic considerations are often more complex than discussed in the literature. This includes the need for the development of robust compliance teams, the struggle with vague terms, and, for example, the absence of industry standards for audits. In addition, the interviews specifically highlight the operational challenges behind content moderation that are not strongly emphasised in the theory. It also appears that the decentralised nature of platform operations and the challenges in communication between different technical teams are important operational challenges not discussed in the literature. Lastly, it appears that there are significant differences in how platforms interpret and comply with the DSA, leading to varying strategies for risk assessments and transparency reports, for example.

In summary, while the theory, largely predictive, highlights the legal and regulatory complexities surrounding the DSA, the interviews offer a deeper insight into the real operational, strategic and compliance challenges faced by platforms. This shows the gap between theoretical discussions and operational reality and highlights the importance of hands-on adjustments within online platforms.

5.3 Implications

The exploration of the challenges faced by online platforms under the DSA reveals an environment characterized by ambiguity, limited resources, and the pace of technological evolution. The results from the interviews and the risk mitigation framework created provide critical insights, illuminating challenges faced by these platforms. They also provide direction for practical application, policy impact and future research directions.

The findings underline a crucial concern, which was also a concern with the GDPR. The DSA's openness to interpretation and lack of concrete guidelines serve as a double-edged sword. On the one hand it offers flexibility, on the other hand it creates an extremely uncertain compliance environment. This

duality raises a fundamental and often asked question in the legislative approach to digital regulation: how do you balance the need for specificity with the changing dynamics inherent in the digital world?

The importance of uncovering challenges from different stakeholders, and providing practical tools for addressing these challenges, lies in their implications for the broader field of digital law and the regulation of online platforms. They underline the urgent need for clearer guidelines, standardized audit frameworks and more robust internal compliance structures within online platforms. These measures are critical not only for navigating the current regulatory landscape, but also for preparing platforms for future legislative developments. The practical applications of these findings provide a blueprint for online platforms striving for DSA compliance and pave the way for more transparent, accountable and secure digital environments.

5.4 Limitations

This research involved consultation with several experts in the field of tech law, IT audit and AI. In addition, discussions were held with two senior program managers within VLOPS. Given this, and the fact that the audit requirement only applies to VLOPS, it can be stated that this research is primarily intended for VLOPS, but also for the European Commission (EC), regulators and auditors. Nevertheless, due to the DSA's step-by-step approach, the findings of this research can also provide new insights for smaller online platforms and other digital services.

Moreover, despite the intentions stated during the interviews, the desired level of detail was not achieved. One reason for this is the confidentiality obligations that interviewees must adhere to due to their professional secrecy. Another reason could be the limited time available to interviewees, especially the program managers within VLOPS. This resulted in follow-up questions being asked to a lesser extent, limiting the depth of information that could be collected. As a result, the internal processes within organizations and their management have not been sufficiently highlighted.

Nevertheless, the sample size of eight interviewed participants provides sufficient basis for the generalization of the research results. The conclusion is based on insights and patterns that emerged from the interviews and which partly align with existing literature and previous research in this area, covering both the GDPR and the DSA. Moreover, when selecting the participants, a strategic choice was made for a broad representation of the target group, which creates an integrated picture of the phenomenon under investigation. However, it should be recognized that a larger and potentially more diverse sample could provide additional insights.

5.5 Suggestions for Future Research

This report, and the DSA itself, offer a wide range of opportunities for future research. As all first-year audit reports and associated assessments will be made public this summer, this provides a valuable opportunity to conduct an analysis of these reports to identify best practices. By comparing the variety of approaches, strategies, and outcomes, one can gain insight into the most effective methods and processes. This can not only contribute to the theoretical knowledge base but can also provide practical guidance for improving future audits.

Another possibility for future research is studying how effective the DSA (Digital Services Act) is in regulating large tech companies and the extent to which it contributes to creating a safer digital environment for users. With this, an in-depth focus could be on content moderation, which is a significant and essential part of the DSA. This research could investigate the methods and techniques used by platforms for content moderation under the DSA, including the challenges related to freedom of expression and censorship.

6 Conclusions & Recommendations

This chapter presents the conclusions of this study, reflecting upon the research rationale and addressing the main research question. It highlights the key findings and discusses the practical contributions of the research. Following the conclusions, the chapter will also offer recommendations, suggesting actionable steps based on the insights gained to further address the challenges identified in this study.

6.1 Conclusions

The Digital Services Act (DSA) is a regulatory framework introduced by the European Union with the objective of creating a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. For online platforms, the DSA mandates comprehensive measures to mitigate the risks associated with illegal content, disinformation, and harmful online behaviour. Platforms are required to implement more effective content moderation systems, ensure transparency in their algorithms, and provide users with more control over the content they see. Moreover, very large platforms face additional scrutiny, including the need to conduct risk assessments and independent audits.

This broad array of requirements presents significant challenges for online platforms. In an effort to delve deeper into the experiences of online platforms striving for compliance with the DSA, the following research question has been formulated:

‘How can expert opinions be leveraged to deepen our understanding of the legal and operational challenges online platforms face in complying with the Digital Services Act (DSA), and how can these challenges be effectively addressed?’

To answer the main research question, it is essential to consider the complicated dynamics between legal ambiguity, operational constraints, and the evolving digital landscape. Insights from expert interviews highlight the need for a multi-faceted approach to effectively navigate these complexities.

The biggest challenge online platforms currently face is the struggle with vague terms, ambiguities, and the absence of clear guidelines, leading to compliance uncertainty. Consultations with digital law, risk and compliance experts are proving instrumental in clarifying these open-ended provisions of the DSA. Experts in this area are of great help to platforms stuck in the ambiguity of terms such as diligent, objective, proportionate'. Relying on legal advice here not only helps in sifting through and translating the law, but also plays a crucial role in shaping compliance strategies that meet both the spirit and the letter of the law. In addition, this challenge calls for proactive collaboration with regulators to advocate for more guidelines in areas such as risk assessments, independent audits, where there is not really an industry standard yet. In this way, an environment can be formed where guidance is both accessible and practical.

Another big challenge is the difficulty platforms have in gaining a holistic understanding of operations due to decentralised structures and rapid development cycles. The formation of internal compliance frameworks is a crucial measure for this and highlights the importance of centralised leadership in navigating different regulatory environments. Such frameworks can ensure a harmonised interpretation of DSA across departments, reducing the risks associated with inconsistent applications and strategic misalignments. Here, an emphasis on training and the creation of cross-functional teams can reduce the gap between technical activities and compliance tasks, ensuring a coherent approach to meeting DSA requirements.

Another challenge, as to be expected in a regulation of this size, is the scarcity of resources and the need for specialised expertise. This can be addressed through strategic allocation of resources and training or recruiting internal and external specialists. But here again, cross-functional compliance teams or partnerships with advisory firms can play a role.

Content moderation, one of the main components of the DSA, poses another challenge. Balancing content with freedom of expression has always been a challenge or trade-off here, and opinions remain divided on this. However, online platforms do experience a challenge with organising content moderation internally, especially with the volume, variety, and complexity of user-generated content. Here, investments in technology, for content moderation in scalable moderation strategies and advanced detection technologies, and system functionality in general, are seen as essential for adapting to the strict requirements of the DSA.

On a broader scale, the maze of multiple global current and future regulatory frameworks calls for a unified compliance framework within these organisations. This not only streamlines the compliance process, but also ensures efficiency and consistency across different legal landscapes.

Linking these findings to the main research question shows that the key legal and operational challenges faced by online platforms in DSA regulation can indeed be effectively addressed. Adopting strategic, informed approaches based on expert insights is likely to pave the way to compliance, balancing legal requirements and operational feasibility.

In conclusion, cooperation between online platforms, the European Commission and auditors is paramount. Online platforms need to embrace a culture of compliance, supported, for example, by robust internal frameworks and technological investments. The European Commission is tasked with providing clear, actionable guidelines to demystify DSA requirements. Meanwhile, auditors play a crucial role in establishing standardised practices that ensure consistency and reliability in compliance assessments.

By following these recommendations, stakeholders can collectively create a digital ecosystem that not only ensures user rights, but also promotes innovation and fair competition. The study thus confirms that the key research question has been answered and provides a first comprehensive blueprint for navigating the complex regulatory landscape shaped by the DSA.

6.2 Recommendations

The primary outcomes of this study, which are the recommendations for online platforms, have been extensively discussed in the final chapters. In summary, these recommendations advocate for more guidance and a proactive approach towards regulators and auditors. They emphasize the development of clear compliance guidelines and a robust internal compliance framework. Additionally, they highlight the importance of enhancing documentation, transparency, and collaboration across teams, investing in technology and in-house expertise, and beginning audit preparations early.

The findings of this study also reveal that there are opportunities for the EC and National Regulatory Authorities. These bodies should focus on issuing detailed guidelines and, in doing so, can provide examples on how to approach certain articles and the legislation as a whole. In doing so, to reduce the ambiguity faced by platforms, it can also release frameworks similar to those developed for the GDPR. Such measures would promote a consistent application of the regulations across various platforms.

Moreover, these bodies should enhance their engagement with stakeholders. By doing so, they can facilitate discussions with online platforms, auditors and, for example, legal experts. The feedback from these discussions can be utilized to refine the implementation process. Here, developing and

communicating clear audit standards form a critical aspect. There should be a structural collaboration with auditors to develop clear and standardised audit protocols for effective monitoring and compliance with the DSA.

In addition, while this research shows that enforcement of the DSA is going to be a crucial part of the success of the legislation, it appears that the EC and other national enforcement agencies have what some describe as a structural shortage of manpower and expertise. The only correct advice that can be given on this is to increase enforcement capacity, recruiting staff with the right competences to effectively oversee the DSA.

For auditors, the recommendation to collaborate with stakeholders to establish clearer standards and standardized audit processes remains pertinent. However, the uncertainties in the DSA and the challenges platforms face also present significant opportunities for audit organisations. These uncertainties require specialised knowledge in digital law and expertise from risk, control, and compliance perspectives. This scenario presents a significant business opportunity for advisory services, not only in relation to the DSA but also in anticipation of forthcoming digital regulations, including the AI Act.

Based on these opportunities, the advice to auditors is to conduct a thorough market analysis on the need for specialised advisory services in digital law, risk management and compliance strategies. Should this analysis confirm a viable opportunity, it will be crucial to train personnel and accumulate expertise at these intersections. This strategic preparation is essential for establishing a leading position in the market for digital compliance.

References

1. decade, E.s.d., *Shaping Europe's digital future.* 2023.
2. Spiekermann, S., & Korunovska, J., *Towards a value theory for personal data.* Journal of Information Technology, 2017. **32**: p. 62–84.
3. Albrecht, J.P., *How the GDPR will change the world.* European Data Protection Law Review, 2016. **2**(3): p. 287-289.
4. Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F., *The Digital Services Act: An analysis of its ethical, legal, and social implications.* Law, Innovation and Technology, 2023. **15**: p. 83-106.
5. Coulter, M., *Big Tech braces for EU Digital Services Act regulations*, in *Reuters*. 2023.
6. Rovilos, V., & Zanfir-Fortuna G. , *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR* Future of Privacy Forum, 2023.
7. N.V., K., *KPMG N.V. Integrated report 2020/2021*. 2022.
8. Statista. *Revenue of the Big Four accounting/audit firms worldwide in 2023*. 2023; Available from: https://www-statista-com.ezproxy2.utwente.nl/statistics/250479/big-four-accounting-firms-global-revenue/.
9. Kitchenham, B., *Procedures for performing systematic literature reviews.* Keele University, 2004.
10. Adeoye-Olatunde, O.A. and N.L. Olenik, *Research and scholarly methods: Semi-structured interviews.* JACCP: JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY, 2021. **4**(10): p. 1358-1367.
11. Safari, B.A., *INTANGIBLE PRIVACY RIGHTS: HOW EUROPE'S GDPR WILL SET A NEW GLOBAL STANDARD FOR PERSONAL DATA PROTECTION.* 2017.
12. Supervisor, E.D.P., *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union."* 2011.
13. Supervisor, E.D.P., *The history of the General Data Protection Regulation.* European Data Protection Supervisor, 2018.
14. Tikkinen-Piri, C., A. Rohunen, and J. Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies.* Computer Law and Security Review, 2018. **34**(1): p. 134-153.
15. Union, E.C.H.F.P.o.t.E. *GDPR checklist for data controllers*. 2020; Available from: https://gdpr.eu/checklist/.
16. Commission, E. *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. 2023; Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.
17. Council, E.P.a., *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)*, E. Commission, Editor. 2022.
18. project, E.I.I.p.c., *DIGITAL SERVICES ACT ensuring a safe and accountable online environment.* European Union Intellectual Property Office (EUIPO), 2023.
19. Commission, E. *Commission designates second set of Very Large Online Platforms under the Digital Services Act*. 2023; Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763.
20. Council, E.P.a., *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422)*. 2003.
21. Council, E.P.a.E., *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*. 2000.

22. Machado, P., et al. *A systematic study on the impact of GDPR compliance on Organizations*. in *ACM International Conference Proceeding Series*. 2023.
23. Almeida, J., P.R. da Cunha, and A.D. Pereira. *GDPR-Compliant Data Processing: Practical Considerations*. in *Lecture Notes in Business Information Processing*. 2022.
24. Altorbaq, A., F. Blix, and S. Sorman. *Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR*. in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*. 2018.
25. Andraško, J. and M. Mesarčík, *Quo vadis open data?* Masaryk University Journal of Law and Technology, 2018. **12**(2): p. 179-220.
26. Bampoulidis, A., et al. *Practice and Challenges of (De-)Anonymisation for Data Sharing*. in *14th International Conference on Research Challenges in Information Science (RCIS)*. 2020. Limassol, CYPRUS.
27. da Conceição Freitas, M. and M.M. da Silva. *GDPR and Suppliers in SMEs*. in *Iberian Conference on Information Systems and Technologies, CISTI*. 2022.
28. Da Conceicao Freitas, M. and M. Mira Da Silva. *GDPR in SMEs*. in *Iberian Conference on Information Systems and Technologies, CISTI*. 2018.
29. de Carvalho, R.M., et al., *Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects.* SN Computer Science, 2020. **1**(4).
30. DePaula, N., et al., *Challenges for social media: Misinformation, free speech, civic engagement, and data regulations.* Proceedings of the Association for Information Science and Technology, 2018. **55**(1): p. 665-668.
31. Duncan, A. and D.A. Joyner. *With or without EU: Navigating GDPR Constraints in Human Subjects Research in an Education Environment*. in *L@S 2021 - Proceedings of the 8th ACM Conference on Learning @ Scale*. 2021.
32. Garrison, C. and C. Hamilton, *A comparative analysis of the EU GDPR to the US's breach notifications.* Information and Communications Technology Law, 2019. **28**(1): p. 99-114.
33. Grundstrom, C., et al. *Making sense of the general data protection regulation-four categories of personal data access challenges*. in *Proceedings of the Annual Hawaii International Conference on System Sciences*. 2019.
34. Härting, R.C., et al. *Impacts of the New General Data Protection Regulation for Small- and Medium-Sized Enterprises*. in *Advances in Intelligent Systems and Computing*. 2021.
35. Hirvonen, P. *Organisational GDPR Investments and Impacts*. in *European Conference on Information Warfare and Security, ECCWS*. 2023.
36. Jantti, M. *Studying Data Privacy Management in Small and Medium-Sized IT Companies*. in *Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020*. 2020.
37. Kumar, A. and P.L. Mehta. *Architectural Framework for Good Data: A Realm for General Data Protection Regulation*. in *International Symposium on Wireless Personal Multimedia Communications, WPMC*. 2018.
38. Labadie, C. and C. Legner, *Building data management capabilities to address data protection regulations: Learnings from EU-GDPR.* Journal of Information Technology, 2023. **38**(1): p. 16-44.
39. Lakshmi, K.K., H. Gupta, and J. Ranjan. *Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges*. in *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*. 2020.
40. Li, Z.S., et al., *Towards privacy compliance: A design science study in a small organization.* Information and Software Technology, 2022. **146**.
41. Li, Z.S., C. Werner, and N. Ernst. *Continuous requirements: An example using GDPR*. in *Proceedings - 2019 IEEE 27th International Requirements Engineering Conference Workshops, REW 2019*. 2019.

42. Mangini, V., I. Tal, and A.N. Moldovan. *An empirical study on the impact of GDPR and right to be forgotten - Organisations and users perspective*. in *ACM International Conference Proceeding Series*. 2020.
43. Mansfield-Devine, S., *Data protection: prepare now or risk disaster.* Computer Fraud and Security, 2016. **2016**(12): p. 5-12.
44. Marotta, A. and S. Madnick. *A Framework for Investigating GDPR Compliance Through the Lens of Security*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2021.
45. Martins, F., L. Amaral, and P. Ribeiro. *Implementation of gdpr: Learning with a local administration case study*. in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*. 2020.
46. Pedroso, L.M., et al. *How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data*. in *Iberian Conference on Information Systems and Technologies, CISTI*. 2021.
47. Politou, E., E. Alepis, and C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions.* Journal of Cybersecurity, 2018. **4**(1).
48. Sirur, S., J.R.C. Nurse, and H. Webb. *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*. in *Proceedings of the ACM Conference on Computer and Communications Security*. 2018.
49. Urban, T., et al. *"Your hashed IP address: Ubuntu." Perspectives on transparency tools for online advertising*. in *ACM International Conference Proceeding Series*. 2019.
50. Usman, M., et al. *Compliance Requirements in Large-Scale Software Development: An Industrial Case Study*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020.
51. Waidelich, L. and T. Schuster. *Privacy Pattern Catalog Approach for GDPR Compliant Appliance: From Legal Requirements to Technology Design*. in *Lecture Notes in Business Information Processing*. 2023.
52. Wiefling, S., J. Tolsdorf, and L. Lo Iacono. *Data Protection Officers' Perspectives on Privacy Challenges in Digital Ecosystems*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2023.
53. Amankwah, J. and N. Stroobants, *GDPR and the Processing of Health Data in Insurance Contracts: Opening a Can of Worms?*, in *AIDA Europe Research Series on Insurance Law and Regulation*. 2022. p. 173-227.
54. Biswal, S.P. and M.S. Kulkarni, *Implications of GDPR on Emerging Technologies in Healthcare.* Cardiometry, 2022(23): p. 255-262.
55. Georgiou, D. and C. Lambrinoudakis. *GDPR Compliance: Proposed Guidelines for Cloud-Based Health Organizations*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020.
56. Lopes, I.M. and P. Oliveira. *Implementation of the general data protection regulation: A survey in health clinics*. in *Iberian Conference on Information Systems and Technologies, CISTI*. 2018.
57. Manescu, D.M. *Personal Data between Individual Protection and the General Interest*. in *4th International Conference on Economics and Social Sciences*. 2021. Bucharest Univ Econ Studies, ELECTR NETWORK.
58. Poritskiy, N., F. Oliveira, and F. Almeida, *The benefits and challenges of general data protection regulation for the information technology sector.* Digital Policy, Regulation and Governance, 2019. **21**(5): p. 510-524.
59. Haddara, M., A. Salazar, and M. Langseth. *Exploring the impact of GDPR on big data analytics operations in the E-commerce industry*. in *Procedia Computer Science*. 2023.

60. Ioan, G.C. *THE NEW ERA OF PERSONAL DATA IN EUROPE: HOW CAN COMPANIES COMPLY?* in *6th International Academic Conference on Strategica - Challenging the Status Quo in Management and Economics*. 2018. Bucharest, ROMANIA.
61. Larsson, A. and P. Lilja, *GDPR: What are the risks and who benefits?*, in *The Digital Transformation of Labor (Open Access): Automation, the Gig Economy and Welfare*. 2019. p. 187-199.
62. Layton, R. and S. Elaluf-Calderwood. *A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices*. in *2019 12th CMI Conference on Cybersecurity and Privacy, CMI 2019*. 2019.
63. Lioudakis, G.V., et al. *Facilitating GDPR Compliance: The H2020 BPR4GDPR Approach*. in *IFIP Advances in Information and Communication Technology*. 2020.
64. Mone, V. and C.L.V. Sivakumar, *An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies.* Legal Information Management, 2022. **22**(3): p. 166-174.
65. Rossi, A., et al. *Challenges of protecting confidentiality in social media data and their ethical import*. in *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*. 2022.
66. Tziogas, C. and N. Tsolakis. *The Dawn of GDPR: Implications for the Digital Business Landscape*. in *Springer Proceedings in Business and Economics*. 2019.
67. Santos-Pereira, C., et al. *Are the healthcare institutions ready to comply with data traceability required by GDPR? A case study in a Portuguese healthcare organization*. in *HEALTHINF 2020 - 13th International Conference on Health Informatics, Proceedings; Part of 13th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2020*. 2020.
68. Li, H., L. Yu, and W. He, *The Impact of GDPR on Global Technology Development.* Journal of Global Information Technology Management, 2019. **22**(1): p. 1-6.
69. Haque, A., et al., *GDPR Compliant Blockchains-A Systematic Literature Review.* Ieee Access, 2021. **9**: p. 50593-50606.
70. Huth, D., A. Faber, and F. Matthes. *Towards an understanding of stakeholders and dependencies in the EU GDPR*. in *MKWI 2018 - Multikonferenz Wirtschaftsinformatik*. 2018.
71. Kulesza, J. *Transboundary data protection and international business compliance*. in *International Data Privacy Law*. 2014.
72. Pathak, P., et al. *Assessment of Compliance of GDPR in IT Industry and Fintech*. in *Lecture Notes in Networks and Systems*. 2023.
73. Zdravkova, K. *Privacy of crowdsourcing educational platforms in the light of new EU regulations*. in *CEUR Workshop Proceedings*. 2019.
74. Agyei, E.E.Y.F. and H. Oinas-Kukkonen. *GDPR and Systems for Health Behavior Change: A Systematic Review*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020.
75. Bertolaccini, L., et al., *The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database.* European journal of cardio-thoracic surgery : official journal of the European Association for Cardio-thoracic Surgery, 2023. **64**(3).
76. Switala, K. *Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy*. in *2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings*. 2023.
77. Shah, A., et al. *Analyzing the impact of GDPR on storage systems*. in *11th USENIX Workshop on Hot Topics in Storage and File Systems, HotStorage 2019, co-located with USENIX ATC 2019*. 2019.
78. Bharti, S.S. and S.K. Aryal, *The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: challenges to the companies.* Journal of Contemporary European Studies, 2023. **31**(4): p. 1391-1402.

79. Bouçanova, C., J.L. Reis, and J.C. Vieira, *Digital marketing and the new age of personal data protection: The case of advertising agencies in Portugal.* RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020. **2020**(E35): p. 141-151.
80. Gruschka, N., et al. *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*. in *IEEE International Conference on Big Data (Big Data)*. 2018. Seattle, WA.
81. Han, S. and S. Park, *A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review.* IEEE Access, 2022. **10**: p. 103888-103905.
82. Nabbosa, V.L. and R. Iftikhar. *Digital retail challenges within the EU: Fulfillment of holistic customer journey post GDPR*. in *ACM International Conference Proceeding Series*. 2019.
83. Piras, L., et al. *DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2019.
84. Cochrane, L., L. Jasmontaite-Zaniewicz, and D. Barnard-Wills, *Data protection authorities and their awareness-raising duties under the gdpr: The case for engaging umbrella organisations to disseminate guidance for small and medium-size enterprises.* European Data Protection Law Review, 2020. **6**(3): p. 352-364.
85. Georgiou, D. and C. Lambrinoudakis, *Compatibility of a security policy for a cloud-based healthcare system with the eu general data protection regulation (Gdpr).* Information (Switzerland), 2020. **11**(12): p. 1-19.
86. El-Gazzar, R. and K. Stendal, *Examining how GDPR challenges emerging technologies.* Journal of Information Policy, 2021. **10**: p. 238-276.
87. Đurović, M. and T. Kniepkamp, *Good advice is expensive–bad advice even more: the regulation of online reviews.* Law, Innovation and Technology, 2022. **14**(1): p. 128-156.
88. Greif, E. and T. Grosz, *To see, or not to see: Online job advertisement and EU non-discrimination law.* European Labour Law Journal, 2023. **14**(3): p. 376-390.
89. Hacker, P., *Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law.* European Law Journal, 2021.
90. Morozovaite, V., *Hypernudging in the changing European regulatory landscape for digital markets.* Policy and Internet, 2023. **15**(1): p. 78-99.
91. Rudohradská, S. and D. Trescáková, *PROPOSALS FOR THE DIGITAL MARKETS ACT AND DIGITAL SERVICES ACT - BROADER CONSIDERATIONS IN CONTEXT OF ONLINE PLATFORMS*, in *EU 2021 - THE FUTURE OF THE EU IN AND AFTER THE PANDEMIC*. 2021. p. 487-500.
92. Bayer, J., *Procedural rights as safeguard for human rights in platform regulation.* Policy and Internet, 2022. **14**(4): p. 755-771.
93. Duivenvoorde, B. and C. Goanta, *The regulation of digital advertising under the DSA: A critical assessment.* Computer Law and Security Review, 2023. **51**.
94. Pakutinskas, P. and T.L. Šepetys, *Algorithmic Parody Protection in the European Union: CDSM Directive and DSA Regulation Perspective.* Baltic Journal of Law and Politics, 2023. **16**(1): p. 79-104.
95. Mazúr, J. and B. Gramblička, *NEW REGULATORY FORCE OF CYBERSPACE: THE CASE OF META'S OVERSIGHT BOARD.* Masaryk University Journal of Law and Technology, 2023. **17**(1): p. 3-32.
96. Farrand, B., *'Is This a Hate Speech?' The Difficulty in Combating Radicalisation in Coded Communications on Social media Platforms.* European Journal on Criminal Policy and Research, 2023. **29**(3): p. 477-493.
97. Kucina, I. and P. Univ Latvia, *EFFECTIVE MEASURES AGAINST HARMFUL DISINFORMATION IN THE EU IN DIGITAL COMMUNICATION*, in *NEW LEGAL REALITY: CHALLENGES AND PERSPECTIVES. II*. 2022. p. 143-155.
98. Mezei, K. and B. Szentgáli-Tóth, *SOME COMMENTS ON THE LEGAL REGULATION ON MISINFORMATION AND CYBER ATTACKS CONDUCTED THROUGH ONLINE PLATFORMS.* LEXONOMICA, 2023. **15**(1): p. 33-52.

99. Reviglio, U. and G. Santoni, *Governing Platform Recommender Systems in Europe: Insights from China.* Global Jurist, 2023. **23**(2): p. 151-181.
100. Dumancic, K., *THE EU REGULATORY ACTIVITIES IN THE AREA OF DIGITAL PLATFORMS AND SERVICES PROVISION*, in *EU 2021 - THE FUTURE OF THE EU IN AND AFTER THE PANDEMIC*. 2021. p. 688-705.
101. Alminen, J.S., et al., *Digital Platforms as Second-Order Lead Firms: Beyond the Industrial/Digital Divide in Regulating Value Chains.* EUROPEAN REVIEW OF PRIVATE LAW, 2022. **30**(6): p. 1059-1088.
102. O'Callaghan, P., et al., *The right to freedom of thought: an interdisciplinary analysis of the UN special rapporteur's report on freedom of thought.* International Journal of Human Rights, 2023.
103. Nóra Kiss, L., *EU Soft Power: Digital Law*, in *Digital Development of the European Union: An Interdisciplinary Perspective*. 2023. p. 265-275.
104. Rodríguez de las Heras Ballell, T., *The background of the Digital Services Act: looking towards a platform economy.* ERA Forum, 2021. **22**(1): p. 75-86.
105. Huckova, R. and M. Semanova, *THE POSITION AND REGULATION OF GATEKEEPERS IN THE CONTEXT OF THE NEW EUROPEAN LEGISLATION*, in *RECOVERY OF THE EU AND STRENGTHENING THE ABILITY TO RESPOND TO NEW CHALLENGES - LEGAL AND ECONOMIC ASPECTS*. 2022. p. 509-526.
106. Blumberg, B., Cooper, D. R. & Schindler, P. S. , *Business Research Methods: Second European Edition.* 2008.
107. Magaldi, D., & Berler, M. , *Semi-structured interviews.* In Springer eBooks, 2020: p. 4825–4830.
108. Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. , *Saturation in Qualitative Research: exploring its conceptualization and operationalization.* Quality & Quantity, 2017. **52**(1893–1907).
109. Cate, F.H., *The EU data protection directive, information privacy, and the public interest.* Iowa L. Rev., 80, 431. , 1994.
110. Bennett, C.J., *Regulating privacy: Data protection and public policy in Europe and the United States.* Cornell University Press, 1992.
111. Hendrickx, F., *Protection of workers' personal data: General principles; 2.1 Global Perspective (By International Labour Organization).* 2022.
112. Council, T.E.P.a.t.E., *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Official Journal L 201 , 31/07/2002, 2002: p. 37-48.
113. Patil, V.T. and R.K. Shyamasundar. *Efficacy of GDPR's Right-to-be-Forgotten on Facebook*. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2018.

Appendix

Appendix A: History of Data Protection and Analysis of GDPR Requirements

In the first part, this appendix discusses the history of data protection in the EU, in the second part the chapters and articles from the GDPR are analysed, after which they are combined in a table.

The history of data privacy and protection in the EU

To understand the impact of data protection regulation on online platforms in the EU, we need to go back to the first forms of digital regulation. The roots of data privacy and protection in the European Union can be traced back to the 1970s when concerns about the use of personal data began to emerge [109].During this time, countries in the EU recognized the need for regulations to safeguard individual privacy in the face of increasing data processing activities [110]. These concerns ultimately lead to the adoption of Treaty 108, which is officially known as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. This is an international agreement established on January 28, 1981, to protect individuals against possible misuse of their personal data during collection and processing. It aims to regulate the cross-border flow of personal data and ensure safeguards for sensitive information. The convention additionally gives individuals the right to know and correct their stored data. Exceptions to these rights are only permitted in cases of essential interests, such as state security. Furthermore, the treaty limits the transfer of personal data to countries that do not have similar legal protection (Treaty No. 108, 1985). This treaty is considered as the foundational framework for the modern data protection measures that remain in force today.

The Data Protection Directive (1995)

National European actions to this convention were somewhat dispersed [111]. While seeing the growing impact of digitalization on society, the European Union took the initiative to adopt legislation in 1995: The Data Protection Directive or Directive 95/46/EC. This legislation aimed to harmonize data protection regulations in the Member States. It established fundamental principles for the processing of personal data and granted specific rights to individuals regarding the collection and use of their personal data.

The ePrivacy Directive (2002)

In 2002, the EU took a further step in addressing privacy concerns by adopting the Directive on Privacy and Electronic Communications, commonly referred to as the ePrivacy Directive [112]. This directive complemented the Data Protection Directive, focusing specifically on issues related to electronic communications. It introduced specific rules regarding the processing of personal data in the context of electronic communications services, including provisions on confidentiality, consent requirements for cookies, and mechanisms to control direct marketing.

Technological Advancements and the Need for Reform

As technology rapidly advanced in the early 21st century, new challenges emerged in the realm of data protection [11]. The increasing prevalence of the internet, e-commerce, and social media raised concerns about the adequacy of existing regulations to address the complexities of digital data processing. An update of regulations was needed, the European Data Protection Supervisor recognised this and published an opinion on the European Commission in June 2011 [12]. This kickstarted the reform of the EU's 1995 Data Protection Directive to strengthen online privacy rights and boost Europe's digital economy. After several years and multiple recommendations and updates, the European Parliament, Council, and Commission reached an agreement on the reformation of the GDPR, and 2 years later, on May 25, 2018, it came into effect [13].

The General Data Protection Regulation (GDPR)

Online platforms, ranging from social media giants to e-commerce websites, often find themselves at the epicentre of GDPR compliance due to their nature as personal data-intensive companies. The

regulation not only requires these platforms to obtain clear and explicit consent before collecting and processing user data but also mandates transparent communication regarding the purpose and duration of data processing [14].

To explore the challenges encountered by online platforms in this study, it is crucial to establish a clear understanding of the essential conditions which are necessary for GDPR compliance. To achieve this, this paragraph provides a comprehensive overview of the GDPR requirements that apply to online platforms since its implementation in 2018.

Summarizing and presenting every detail of articles in the GDPR is an extensive task that falls beyond the scope of this research. This is why, in this paragraph, we will focus on identifying and highlighting important changes from the preceding regulation that are relevant to online platforms. To accomplish this, we draw upon the legal provisions outlined in the GDPR and leverage insights provided by Machado et al. (2023), [22]. Their research explains the changes and implications introduced by the GDPR in comparison to its predecessor.

To maintain clarity in this section, the requirements are organized in the same sequence as the articles outlined in the GDPR. In this analysis, Chapters VI, VII, IX, and X of the GDPR have been left out as they delve into matters concerning the independent supervisory authorities of member states, along with the cooperation and consistency between them. Given the focus on online platforms, these chapters are considered irrelevant to the scope of this study.

Chapter I & II General Provisions & Principles

Article 3: Extended territorial scope

The GDPR starts with introducing an extended territorial scope. This extended territorial scope applies to controllers and processors based in the EU, irrespective of where the processing occurs. It encompasses personal data processing related to goods or services offered to data subjects in the EU and the monitoring of data subjects' behaviour within the EU.

Articles 4-11: New definitions, principles, and conditions

New definitions introduced by the GDPR, that are relevant for data intensive companies and thus online platforms include pseudonymisation, genetic data, biometric data, data concerning health, binding corporate rules, and personal data breach. These new definitions along with other important definitions, like the meaning of (sensitive) personal data, controller, and processor can be found in Appendix 1 ‘Abbreviations and definitions’.

Next to these definitions, the GDPR introduces new provisions and principles, emphasizing transparency of data processing and accountability (article 5), and processing that does not require identification (article 11). In addition, some already existing provisions and principles have been clarified or specified, including the data minimization principle (article 5), conditions for consent (article 7), and lawfulness of data processing (article 6). The latter now includes specific conditions for the lawful processing of children's personal data, where consent or authorization by the child's parent or custodian is required if the child is younger than 16 years old.

The GDPR, alongside supporting research, designates Article 5 as the cornerstone representing the primary principles that companies are obligated to live up to. These fundamental principles serve as guidelines, shaping the responsible and lawful handling of personal data within the regulatory framework. Table 2 shows the seven key principles of Article 5 of the GDPR.

Table A1 The seven GDPR principles according to article 5.

Principle	Description

Lawfulness, fairness, and transparency	Personal data must be processed lawfully, fairly, and transparently in relation to data subjects
Purpose limitation	Personal data can only be collected for specified, explicit, and legitimate purposes (although further processing for the purposes of public interest, scientific or historical research, or statistical purposes is not considered incompatible with the initial purposes and is therefore allowed.)
Data minimization	Personal data must be adequate, relevant, and limited to what is necessary for processing
Data accuracy	Personal data must be accurate and kept up to date.
Data storage limitation	Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
Data security	Personal data must be processed in a manner that ensures security.
Data accountability	The controller shall be responsible for, and be able to demonstrate compliance with GDPR principles

Next to these key principles, according to article 6 of the regulation, the processing of personal data is permissible only when there is a legal basis for it. The legal bases for the lawful processing of personal data are when:

(a) the data subject has *given consent to the processing of his or her personal data* for one or more specific purposes;

(b) processing is necessary for *the performance of a contract to which the data subject is party* or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for *compliance with a legal obligation* to which the controller is subject;

(d) processing is necessary in order to *protect the vital interests of the data subject* or of another natural person;

(e) processing is necessary for *the performance of a task carried out in the public interest or in the exercise of official authority* vested in the controller;

(f) processing is necessary for *the purposes of the legitimate interests* pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Chapter III Rights of the Data Subject

Article 12: Transparency and modalities

Article 12 of the GDPR states controllers have new responsibilities, including the obligation to provide transparent, easily accessible, and comprehensible information about the processing of personal data. They are also required to establish procedures and mechanisms that broaden the ways data subjects can exercise their rights. This includes facilitating electronic requests, responding to requests within a specified timeframe, and offering explanations for potential refusals.

Articles 13-15: Information and access to personal data

Article 13-15 obligate controllers to include new information requirements. Controllers must now provide data subjects with additional information about the controller, the data subject's rights, and data transfers to third countries. Additionally, there are added informational requirements concerning the data subject's right of access to their personal data. If personal data are being processed, the data

subject has the right to receive supplementary information regarding the data processing and their associated rights.

Articles 16-20: Rectification and erasure

Articles 16 to 20 specify the rights of the data subject regarding the right to rectification, erasure, and restriction of the processing of personal data. This includes the conditions for the data subject's right to be forgotten and the conditions for the data subject's right to restriction of processing.

In addition, a new right for data subjects has been introduced: the right to data portability from one system to another.

Articles 21-22: Right to object and automated individual decision-making

Article 21 sets out the right to object to the processing of personal data, including profiling, and requires that the right to object be presented clearly and separately from other information. Controllers are required to demonstrate compelling legitimate grounds for processing which override the interests or fundamental rights and freedoms of the data subject, with the burden of proof remaining with the controller.

Article 22 adds that the data subject has the right not to be subject to a decision based on automated processing. Such decisions are only permitted if they are based on a contract between the data subject and the controller or on the basis of the data subject's explicit consent.

Chapter IV Controller and Processor

Articles 24-31: General obligations

Under the GDPR the controller's responsibilities now encompass new foundations, specifically the principles of data protection by design and by default, also referred to as privacy by design or PBD (article 25).

Further clarifications have been provided regarding controllers' responsibilities and obligations. This includes addressing situations involving multiple joint controllers and specifying the position and obligations of processors in the context of personal data processing under the authority of controllers.

Articles 31 and 31 impose additional obligations on controllers and processors. It states they must keep a register of the processing activities under their responsibility and actively cooperate with the supervisory authority. In particular, controllers and processors not established in the EU are obliged, under certain conditions, to appoint a representative within the EU.

Articles 32-34: Security of personal data

Articles 32 to 34 describe data security and extend the scope of obligations to processors where previously they were only controllers. The articles provide clarifications on the implementation of security measures for data processing and specifically outline the obligations of data processors.

A new obligation for data controllers includes mandatory notification of a personal data breach to both the supervisory authority and the data subject. Similarly, a new obligation is imposed on processors, necessitating notification of a personal data breach to the controller.

Articles 35-36: Data protection impact assessment and prior consultation

Under these articles, controllers now have a new obligation, which necessitates the completion of a data protection impact assessment (DPIA) before engaging in potentially risky processing activities.

In addition, A simplification has been introduced regarding the consent of controllers to process personal data. In particular, prior consultation with the supervisory authority is only mandatory if the

data protection impact assessment shows that there is a high risk associated with the data processing or if the supervisory authority considers this necessary.

Articles 37-39: Data protection officer

Another new obligation, applying to both controllers and processors, involves the appointment of a Data Protection Officer (DPO). This requirement comes into play when data processing operations entail regular and systematic monitoring of data subjects or when processing special categories of data. The GDPR outlines the core tasks of the DPO in article 39, these activities include informing and advising the controller, processor or employees, monitoring compliance with the GDPR and collaborating with the supervisory authority.

Articles 40-43: Codes of conduct and certification

Articles 40 to 43 contain simplifications regarding the adoption of codes of conduct. Now supervisory authorities can directly approve codes of conduct at national level.

In addition, new methods have been introduced to demonstrate GDPR compliance with processing activities. These include data protection certification mechanisms, seals and markings.

Chapter V Transfers of Personal Data to Third Countries

Articles 44-49: Transfer principles and binding corporate rules

Articles 44 until 49 establish new conditions for personal data transfers, introducing Binding Corporate Rules (BCRs), an approved code of conduct, and an approved certification mechanism as new methods of ensuring appropriate safeguards for the transfer of personal data to third countries or international organizations.

Chapter VIII Remedies, Liability and Penalties

Articles 77-84: Rights and general conditions

Articles 77 to 84 shed light on the data subject's right to a legal remedy. the GDPR allows the data subject to lodge a complaint with a supervisory authority if he or she believes that the processing of his or her data infringes the GDPR. The regulation also specifies that entities, organizations, and associations are authorized to file a complaint on behalf of the data subject.

In addition to this, liability has been extended to processors, making both the controller and the processor liable for any damage suffered by the data subject as a result of processing that infringes the GDPR. Continuing on this, the liability of joint controllers and joint processors has been clarified. Each controller and processor are now collectively responsible for the full damage suffered by the data subject.

The GDPR also introduces administrative fines that can be imposed by supervisors on both the controller and the processor. These fines serve as sanctions for violations of the GDPR, as an illustration, a violation of GDPR principles, such as the data minimization principle, may result in a fine of up to €20 million or 4% of the total annual worldwide turnover for an organization, whichever amount is higher.

Summary of GDPR requirements

To provide a more comprehensive picture of the implications for online platforms when handling personal data, we have summarized the GDPR requirements in Table 3, which also answers sub-question one of this study. This table takes a closer look at four crucial aspects of the GDPR: legal basis and transparency, data security, liability and governance, and privacy rights. The data used to compile this table comes directly from the GDPR legal text and is then supplemented with information from the European Commission. This table provides insight into the requirements that companies must

meet, and therefore gives us sufficient tools to search the literature for challenges that companies experience with GDPR compliance.

Table A2 Summarized GDPR requirements.

Requirement	Brief Explanation
	Lawful basis and Transparency
Information Audit	Organizations, especially those with 250 or more employees, must maintain an updated list of processing activities, including purposes, data types, access details, third-party involvement, data protection measures, and deletion plans.
Legal Justification	Data processing must align with one of the six conditions in Article 6 of the GDPR. Additional provisions for children and special categories of personal data (Articles 7-11) should be considered. Legal bases must be documented, especially if relying on "consent" or "legitimate interests."
Privacy Policy	Clear and concise information about data processing and legal justification must be provided in the privacy policy. The information should be easily accessible and understandable, particularly for children.
	Data Security
Data Protection by Design and Default	Organizations must integrate data protection principles into product development and data processing, implementing appropriate technical and organizational measures. Encryption, pseudonymization, and adherence to Article 5 principles are essential.
Encryption, Pseudonymization	Utilize encryption, pseudonymization, or anonymization of personal data wherever possible, especially in widely used productivity tools that offer end-to-end encryption.
Internal Security Policy	Establish an internal security policy covering email security, passwords, two-factor authentication, device encryption, VPN usage, and provide training to ensure team members are knowledgeable about data security.
Data Protection Impact Assessment	Perform a data protection impact assessment whenever processing activities pose a high risk to individuals' rights and freedoms. Have a process in place to analyse and minimize risks.
Data Breach Notification	In the event of a data breach, notify the supervisory authority within 72 hours and communicate breaches to data subjects promptly, unless the breach is unlikely to put them at risk. Authorities in non-EU countries may include the Office of the Data Protection Commissioner in Ireland.
	Accountability and Governance
GDPR Compliance Accountability	Designate a responsible person within your organization to ensure GDPR compliance. This individual should evaluate data protection policies and oversee their implementation.
Data Processing Agreement	Sign a data processing agreement with third parties handling personal data on your behalf. These agreements outline rights and obligations for GDPR compliance and should be reviewed for reliability and data protection guarantees.
Appointment of Representative	If your organization is outside the EU and processes data related to individuals in a specific member state, appoint a representative within that country to communicate with data protection authorities.
Data Protection Officer (DPO)	Appoint a Data Protection Officer if required by circumstances or as a proactive measure. The DPO monitors GDPR compliance, assesses data protection risks, advises on impact assessments, and collaborates with regulators.
	Privacy Rights

Right to Information Access	Data subjects have the right to request and receive information about the personal data you have, its usage, storage duration, and the reason for retention. Comply with such requests within a month, and initial copies should be provided for free.
Right to Correct or Update Information	Data subjects can easily correct or update inaccurate or incomplete personal information. Implement a data quality process and facilitate customer access and updates within a month, verifying their identity.
Right to Data Deletion	Data subjects can request the deletion of their personal data, which should be honoured within about a month, except for specific grounds for denial. Identity verification of the requester is necessary.
Right to Stop Data Processing	Data subjects can request to restrict or stop processing their data, honoured within about a month. While processing is restricted, data storage is permitted, and the data subject must be notified before resuming processing.
Right to Data Portability	Data subjects can receive a copy of their personal data in a transferable format. Ensure the ability to send data in a commonly readable format upon request.
Right to Object to Data Processing	Data subjects can object to data processing, particularly for direct marketing purposes, leading to an immediate cessation of processing unless compelling legitimate grounds exist.
Protection of Rights in Automated Decision-Making	Establish procedures for organizations using automated processes for decisions with legal or significant effects. Provide mechanisms for human intervention, allowing individuals to weigh in on decisions and challenge them.

Appendix B: Explanation of GDPR Specific Challenges

This appendix takes a closer look at the challenges from the literature that companies have experienced in complying with the GDPR.

1) Difficulty with facilitating interoperability and portability across different systems, organizations, and countries.

With 28 mentions, difficulty with facilitating interoperability and portability across different systems, organizations, and countries is another challenge organizations experience while trying to comply with the GDPR.

Starting with the technical challenges, Grundstrom et al. (2019) and Labadie and Legner (2023) highlight the problems arising from the unstructured nature of data and the lack of clear standards. This lack of standardization makes it difficult to ensure portability and maintain data quality. Kumar and Mehta (2018) emphasize the complexity of managing data portability and the complete deletion of user data, noting that companies are required to handle user requests for data portability and deletion within specific timeframes.

From an organizational standpoint, Agyei and Oinas-Kukkonen (2020) stress the importance of allowing data subjects to control their own data, highlighting the challenges related to the ownership and control of health data. This need for control is crucial in healthcare, where patients should own and manage their data in formats that support interoperability. Santos-Pereira, Augusto, and their team (2020) also draw attention to the difficulties organizations face in managing a large number of legacy information systems, some of which are no longer supported by their providers, thereby complicating updates or upgrades.

On the regulatory front, Switala (2023) points out the challenges related to ensuring cross-border interoperability of healthcare solutions. These challenges include harmonizing technical and organizational measures and the differences in regulations regarding medical confidentiality between countries. Achieving interoperability between Electronic Health Record (EHR) systems in EU Member States is particularly challenging due to these regulatory discrepancies. The harmonization of principles observing medical confidentiality is deemed essential for interoperable cross-border processing of medical data.

Furthermore, Garrison and Hamilton (2019) emphasize the added complexity for businesses in aligning their data storage practices with GDPR requirements, especially with the right to data portability. This requires organizations to facilitate the transfer of user data in commonly used file formats. Tikkinen-Piri (2018) adds to this that challenges here include not only the absence of uniform standards but also the risks to other data subjects' privacy and the need for awareness-raising and training programs.

In conclusion, the above-named papers all state that the challenge of facilitating interoperability and portability under the GDPR is significant. It encompasses technical issues like data structure and standardization, organizational hurdles involving data control and legacy systems, and regulatory complexities stemming from differing national laws, especially concerning health data, and the need for harmonization. These challenges are crucial to address for ensuring GDPR compliance and facilitating the smooth and secure flow of data across borders and systems.

2) (Active) Consent management issues.

Active consent management under the GDPR, with 28 different mentions, presents a significant challenge for organizations, encompassing a range of issues from technical and procedural complexities to the difficulties posed by modern technologies like machine learning.

One of the primary challenges, as noted by Almeida et al. (2022), Bharti & Aryal (2023), and Tikkinen-Piri (2018), is the challenge in obtaining explicit and informed consent from users. This difficulty is increased by practices such as the use of pre-ticked boxes and complex forms, and by the GDPR's lack of precise requirements on how to obtain free and informed consent. Organizations are required to implement clear, unambiguous, and affirmative consent mechanisms, along with detailed information presentation and recording procedures. This includes managing specific consent aspects such as cookie approval and consent for children's data processing.

The communication challenges highlighted by Altorbaq et al. (2018) and Grundstrom et al. (2019) emphasize the complexities in ensuring proper consent management, especially when data processing is outsourced. This necessitates effective interaction between controllers, processors, and data subjects, and the need for meaningful consent beyond mere checkbox compliance.

The impact of this challenge can be seen in different sectors, as noted by Bouçanova et al. (2020) and Duncan & Joyner (2021). The first mentioned discusses the impact on digital marketing strategies, particularly in obtaining explicit consent for marketing actions and processing sensitive data. The latter explores the challenges in academic research, particularly in obtaining consent for research surveys, exploring the paradox of obtaining consent when prior consent is required for contact.

El-Gazzar & Stendal (2021) and Pathak et al. (2023) identify consent challenges posed by advanced technologies. The use of machine learning algorithms complicates the process of obtaining informed and unambiguous consent due to the unclear purposes and repurposing of collected data. Similarly, Fintech companies, dealing with biometric and digital authentication systems, face specific challenges in obtaining explicit consent for processing biometric data.

These challenges of active consent management are diverse and substantial, affecting a wide range of sectors. They include ensuring clear and informed consent, adapting to stringent GDPR requirements, managing communication complexities, and integrating consent processes with advanced technologies. Addressing these issues is crucial for organizations to ensure GDPR compliance and protect personal data effectively.

3) Difficulty with operational adaption to PBD, access & authorization management, and business continuity.

The difficulty with operational adaptation to Privacy by Design (PbD), access and authorization management, and business continuity under the GDPR presents a complex array of challenges for organizations. These challenges stem from the need to align day-to-day operations with GDPR's stringent privacy requirements, while maintaining effective business practices and ensuring security and accessibility of personal data.

A common issue, as noted by de Carvalho et al. (2020), H. Li et al. (2019), Lioudakis et al. (2020), and Georgiou & Lambrinoudakis (2020b), is the necessity for organizations to modify their operational practices to comply with GDPR. This includes identifying and extracting personal data, implementing holistic search tools, and efficiently handling customer or employee data requests. Organizations are challenged to identify flaws in their current practices against GDPR requirements and to re-engineer processes for privacy-friendly practices. This requires significant planning and review of people, roles, systems, and processes.

Another aspect of this challenge, highlighted by Georgiou & Lambrinoudakis (2020b) and Urban et al. (2019), relates to balancing access to authorized persons while preventing unauthorized access, a principle tied to the GDPR concept of accountability. This includes preventing unauthorized access through design actions and addressing the cost allocation of privacy. Companies also grapple with

deciding the level of identification required before answering access requests to ensure that access is granted to the correct individual while avoiding the creation of more sensitive data through authentication processes. Furthermore, providing access to personal data for data subjects involves significant manual work and raises concerns about the security of personally stored data and access for legal purposes. Understanding customer boundaries in light of GDPR and managing data flow within the advertising ecosystem, including data exchanges between companies, presents additional operational challenges.

In the specific context of healthcare, as discussed by Georgiou & Lambrinoudakis (2020a), the challenge extends to ensuring healthcare data security within cloud computing environments. This encompasses identity management, access control, internet-based access, authentication, authorization, and concerns related to cybercriminals. They note that maintaining the integrity of data, assuring that digital information stored and transferred in the cloud is uncorrupted and accessible or modifiable only by authorized individuals, is a particularly challenging task.

In conclusion, the challenge of operational adaptation to PbD, access and authorization management, and business continuity is asking a lot from companies. It requires organizations to undertake significant changes in their operational practices, involving not just compliance with privacy regulations but also ensuring security, accessibility, and integrity of data.

4) Difficulty with anonymization, pseudonymization, and encryption of data.

With 16 mentions, another prominent challenge is the difficulty with anonymization, pseudonymization, and encryption. These challenges arise from the need to balance data utility and privacy protection while complying with GDPR requirements.

Industries processing large volumes of data, including "big tech" companies, healthcare, and the finance sector, as mentioned by Larsson & Lilja (2019), face challenges with regard to the careful handling and anonymization of sensitive personal data and ensuring compliance while maintaining the utility of the data.

Rossi et al. (2022) highlight the specific challenges of anonymization and pseudonymization. While anonymization theoretically makes re-identification impossible, it faces challenges, especially with graph data and online content that can be easily re-identified. Next to this it states that pseudonymization offers enhanced data security but requires a risk-based approach to determine its appropriateness in different contexts.

DePaula et al. (2018) and Gruschka et al. (2018) address the ethical concerns and practical challenges in data anonymization. They state a key challenge is striking a balance between utilizing user data for business purposes and respecting user privacy and rights. This involves navigating between providing personalized services and avoiding unethical or intrusive practices. Anonymization operations, while protecting privacy, can result in a loss of information and reduced data utility.

Almeida et al. (2022) and de Carvalho et al. (2020) discuss the challenges associated with data encryption. GDPR emphasizes encryption for data protection, but challenges include choosing secure algorithms, considering computational power, and addressing issues like the efficiency of homomorphic encryption and the limitations of trusted execution environments. Traditional data encryption techniques are deemed unsuitable for the big data paradigm, as they prevent third-party servers from operating over encrypted data. They state that therefore, privacy-preserving techniques compatible with data analytics are needed to perform operations on encrypted data without compromising confidentiality. Marotta & Madnick (2021) add to this by stating the key challenge witch

data encryption lies in the abstract and insufficient ways to protect data, including the frequency of testing and evaluating security measures.

Finally, Haddara et al. (2023) notes the impact of GDPR on data collection and its use in analytics solutions and algorithmic decision-making systems. With GDPR in place, there is a reduction in the amount of data collected, impacting the effectiveness of these systems.

In conclusion, the challenges concerning anonymization, pseudonymization, and encryption of data under GDPR are versatile and significant. They involve ethical considerations, balancing privacy protection with data utility, choosing appropriate techniques, and adapting to the evolving landscape of data processing and analytics. Addressing these challenges is crucial for organizations to ensure GDPR compliance while effectively managing and utilizing their data.

5) Lack of a metric or data management system to check for system security and GDPR compliance.

The lack of a metrics or data management system to monitor system security and GDPR compliance is another challenge organizations face.

Almeida et al. (2022) highlight the difficulty in finding a benchmark for system security and GDPR compliance, highlighting the challenges posed by the ever-evolving nature of vulnerabilities in IT systems. This makes it difficult to establish a consistent and reliable metric that can accurately reflect the security and compliance status of a system.

Bharti & Aryal (2023) discuss the disconnect between legal systems and internet security. This disparity necessitates the development of a capacity model that can bridge the gap between regulatory requirements and technical security measures.

Hut et al. (2018) point out the need for a data privacy management system that supports GDPR compliance. Such a system would ideally provide a framework for monitoring and managing data privacy in accordance with GDPR requirements, but developing and integrating these types of systems comes with its own challenges.

The challenge of not having a metric or data management system for system security and GDPR compliance involves both technical and legal aspects. It requires a comprehensive approach that considers the evolving nature of IT vulnerabilities and the need for alignment between legal and technical frameworks. Addressing this challenge is critical for organizations to ensure continued GDPR compliance and maintain robust system security.

6) Difficulty of applying GDPR principles for AI and ML systems.

The difficulty of applying GDPR principles for AI and ML systems explicitly stated in several articles. It's named in combination with accountability, fairness, purpose limitation, data minimization, and transparency.

A primary concern, as highlighted by both El-Gazzar & Stendal (2021) and Mone & Sivakumar (2022), is the issue of accountability in AI systems. The autonomy of these systems raises questions about whether they should be considered controllers or processors under GDPR. This uncertainty complicates the assignment of responsibility, especially when AI systems make decisions without human intervention.

Another significant challenge is ensuring fairness in ML algorithms. These algorithms may produce discriminatory results due to biased training data, conflicting with the GDPR's fairness principle. Both

El-Gazzar & Stendal (2021) and Mone & Sivakumar (2022) emphasize the potential for discrimination in automated decision-making and profiling, which violates GDPR's fairness principle.

Furthermore, the purpose limitation and data minimization principles of GDPR are challenged by the nature of ML algorithms. El-Gazzar & Stendal (2021) and Mone & Sivakumar (2022) point out that these algorithms may process data for unclear purposes, generating new data, and thus potentially conflicting with GDPR requirements that data be processed for specific, explicit, and legitimate purposes.

The complexity of AI systems, particularly those based on ML algorithms, also poses transparency compliance issues. El-Gazzar & Stendal (2021) adds that the difficulty in explaining AI system logics can hinder transparency and impede the data subject's right to understand processing activities. This is echoed by Mone & Sivakumar (2022), who mention that automation and ML algorithms often do not conform to GDPR articles related to explaining algorithmic logic.

Lastly, Almeida et al. (2022) address the challenge regarding the right to be forgotten in AI. This involves balancing the AI model's learning process with GDPR's requirements for data erasure.

In summary, the challenges of applying GDPR principles to AI and ML systems are intertwined, with key issues surrounding liability, fairness, purpose limitation, data minimization and transparency. Addressing these challenges is essential to ensure that AI and ML technologies comply with the GDPR and protect the rights of data subjects.

7) Lacking data breach communication, lacking a process for timely notification of users and authorities.

The challenge of lacking data breach communication and the process for timely notification of users and authorities is another critical aspect of GDPR compliance. This challenge involves establishing clear procedures for handling data breaches, including notification to data subjects and relevant authorities.

Multiple sources emphasize the importance of defining processes for the communication of data breaches. Loan (2018), Huth et al. (2018), Lakshmi et al. (2020), and Tikkinen-Piri (2018) all highlight the necessity for controllers to have well-established procedures for notifying data protection authorities and data subjects about data breaches as early as possible. This includes the development of clear and well-practiced procedures within organizations to handle possible breaches and related reporting efficiently and effectively.

Marotta & Madnick (2021) address a specific challenge within this requirement: the subjective judgment of whether a data breach represents an actual risk. This subjectivity can lead to negligence in handling data breach incidents, indicating a need for clear guidelines and criteria to assess the severity and risk of data breaches.

In summary, the challenge of lacking data breach communication and timely notification processes is centered around the need for clear, well-defined, and effective procedures within organizations. These procedures are crucial for the prompt and appropriate notification of both data protection authorities and data subjects in the event of a data breach, ensuring compliance with GDPR and minimizing the impact of such incidents.

8) Difficulties with DPIA.

The challenges associated with conducting Data Protection Impact Assessments (DPIAs) under the GDPR are significant for organizations, particularly due to the subjectivity of high-risk processing and the complexity of certain technological environments.

Bouçanova et al. (2020), Loan (2018), and Switala (2023) highlight the requirement of a DPIA for processing activities that may pose high risks to individuals' rights and freedoms. Conducting a DPIA is mandatory for processing likely to result in a high risk, but the challenge lies in the subjectivity of what constitutes high-risk processing, which can vary across regions. This adds complexity to compliance efforts, especially for processes involving systematic and extensive evaluation of personal aspects based on automated processing.

Kulesza (2014) points out that the DPIA, as required by the GDPR, may not adequately address significant privacy threats posed by cloud computing and transboundary data transfers. The suggestion to include cloud services in the list requiring a DPIA and to conduct periodic reviews and public scrutiny reflects the need to address the specific challenges posed by these technologies.

Labadie & Legner (2023) and Tikkinen-Piri (2018) discuss the difficulties organizations face in conducting and documenting in-depth DPIAs, especially for sensitive processing activities involving technologies like Big Data Analytics and AI. The GDPR's accountability principle and documentation requirements mandate the creation of new documentation, including a record of processing activities. Adapting to these new documentation requirements poses challenges, particularly for agile and lean companies, and requires considering specific risks to the business sector and company when conducting assessments.

In conclusion, the difficulties with DPIAs come from the subjectivity of defining high-risk processing, the complex technological environments such as cloud computing and AI, and new documentation requirements. Addressing these challenges is crucial for organizations to ensure compliance with GDPR and to adequately assess and mitigate risks associated with data processing activities.

Appendix C: GDPR Challenges with Less than 5 Mentions

This appendix contains challenges from the SLR on GDPR compliance challenges with fewer than 5 mentions.

Table C1 GDPR Challenges with less than 5 mentions.

Challenge	Source	Total mentions
Finding the balance between utilizing user data for business purposes and respecting privacy rights	[30], [33], [113], [47]	4
Compliance deadline; may 25 2018, coming too soon.	[34], [61], [41]	3
Impact of RTBF on organizations that rely on selling personal data to advertiser (social media)	[32], [113]	2
Lack of commitment of top management for data privacy requirement such as GDPR.	[36], [45]	2
Varying GDPR interpretations by individual countries create challenges for standardized approval, e.g. age or health data	[82], [53]	2
Transition from directive to regulation, making organizations directly responsible	[28]	1
Identity theft risk and online fraud created by GDPR's users right to control data can be exploited by criminals	[62]	1
Data protection fatigue, multiple regulations leading to a complacent attitude towards GDPR compliance.	[43]	1

Appendix D: Participant Preference, Demographic Information, and Interview Guide

This appendix contains the profiles drawn up with the necessary requirements for participants in interviews.

Internal (interviews within the KPMG network)

- Participants must have sufficient experience with both the GDPR and the DSA; participants must have worked with or provided advice on both legislations at least once.
- Participants must have a minimum experience of 2 years in their respective roles related to data privacy or another role at the intersection of law and technology.

External (interviews outside the KPMG network)

- Participants must work within an organization that is obligated to comply with the DSA.
- Participants must have sufficient experience with the DSA; participants must have worked with or provided advice on the DSA at least once.

General Preferences

- Professionals with a minimum of three years of active experience in their roles, related to law and technology.
- Capability to engage in interviews conducted in English.

Below we will show the semi-structured interview guide that will be used to interview experts.

Introduction

- Thank you for agreeing to participate in this interview. The purpose of this interview is to gain a deeper understanding of the challenges organizations face in complying with the GDPR and the DSA. As I mentioned in the email, while the GDPR has been extensively discussed in the literature, this is not the case for the DSA. I would like to discuss these challenges with you and briefly talk about possible solutions at the end.
- May I record this interview? All recordings will be deleted after analysis. If yes, please start recording.
- And two things now that the recording is on:
- Do I have your permission to use the results of this interview for my study? Personal information, as well as possible information about companies or cases, will be anonymized. I also assure you that you can leave the research at any time without explanation.

Background

- First, could you briefly tell me about your role and what it entails?
- How many years of experience do you have in this field?
- Do you have experience working with the GDPR? If so, could you briefly explain in what way, for example, in an advisory role?
- Do you have experience with the DSA? If so, could you briefly explain in what way, for example, in an advisory role?

Challenges for Online Platforms

- Before I introduce any form of bias by mentioning challenges from the literature, what do you think are the biggest challenges that online platforms face in complying with the DSA?
- This could be anything from challenges in the text of the law itself to operational challenges.

Content Moderation

- Literature often discusses the clash between removing content and freedom of speech. What is illegal is often subjective and also varies by country. For example, in the sale of weapons or other means? What is your view on this? How do companies handle this, and how is this reflected on platforms?
- Articles describe that it is difficult to identify forms of illegal content; hate and radicalization in memes or AI-edited political statements. How do companies handle this?
- Some articles suggest that the DSA, as it currently stands, does not go far enough to fully address manipulation by algorithms, profiling, and microtargeting. It emphasizes that the main focus of the DSA is on transparency and risk management for large platforms, creating a gap in coverage for smaller and medium-sized platforms.
- What is your opinion on this, are the measures for the categories other than VLOPS sufficient?

Missing Guidelines and Openness to Interpretation

- Literature mentions for both the GDPR and the DSA that there is a lack of specific requirements and openness to interpretation.
- Is this also the case for the DSA, and if so, can you provide examples?
- E.g., requirements in terms and conditions for the protection of minors. Or terms like simple, user-friendly, easy, clear.
- How do companies deal with this lack of requirements?
- For example, regarding the protection of minors; it states “primarily focused on children”. How do companies handle this? Or do they simply state that this does not apply to them because they do not target minors?
- No profiling allowed if you can be reasonably certain that a recipient of your service is a minor.
- And also, regarding auditors, is there a standard framework to audit DSA compliance?

The Lack of Practical Guidance and Standard Frameworks

- This nearly mirrors missing guidelines, but the lack of practical guidelines and standardized frameworks was also described as a major challenge in implementing the GDPR.
- Does this also apply to the DSA, and can you provide examples?
- Is this the result of the EU's decision to choose speed over quality?
- Will this lack of guidance lead to different interpretations by online platforms, and how will this play out?

Resource Scarcity and Substantial Implementation Cost

- Another challenge mentioned for the GDPR is the lack of resources and the significant implementation costs and time.
- Is this also the case in complying with the DSA?
- Do online platforms have sufficient and appropriate resources to comply with the DSA? And do they have the right expertise? E.g., lawyers.
- DSA legislation is built in stages, so companies of different sizes have more measures.
- How do smaller platforms handle a lack of resources? Or is there just less attention and priority for the DSA within these smaller platforms, since they are not required to conduct an audit?

Emerging Technologies

- Some research describes that it can be difficult to comply with the DSA due to technological evolution and systems and their complex nature. Ensuring transparency and being able to justify the use of Hypernudging techniques poses a significant challenge, especially given their opaque and complex nature. Nudging: Small encouragements in a certain direction to influence choices. And hypernudging is that but through big data and advanced technologies, such as AI, to deliver much more personal and powerful encouragements.
- What is your view on this, and how do you see emerging technologies affecting compliance with the DSA in the future?

Policy Makers

- If we now look from the perspective of a policymaker, what do you think are the main challenges in implementing and enforcing the DSA?
- The GDPR was initially unclear and open for interpretation, do you think this has improved with the introduction of the DSA?
- Do you think the DSA will be consistently implemented and enforced across Europe, or will regional differences arise?
- Research mentions that the EU might fall behind in terms of innovation, due to strict legislation like the DSA. What do you think about this?
- How could the DSA be improved to better meet the needs and realities of different types of online platforms?

Ranking and Unnamed Challenges

- Based on the conversation we just had, what would you name as the 3 biggest challenges that online platforms face?
- Are there challenges that your organization, or an organization to which you have advised, has faced in complying with the DSA that were not discussed in this interview?
- Discuss current developments, and what is coming up?
- What questions do you think I should ask customers according to you?

Closing

- Thank the interviewee for their openness and valuable insights.
- Are you interested in a summary of the research results? If so, should I send this to your email?
- Again, I assure you that your answers will remain confidential. If you have further questions or want to provide additional information, please feel free to contact me.

Appendix E: Interview Transcriptions

Due to the protection of the interviewees' privacy and the traceability of data, it has been decided not to make the interview transcripts public. For more information about these transcripts, you can contact the author of this thesis via email: quinthulshof10@gmail.com.