

# Content analysis of EU directives and regulations: legislative frameworks and consumer rights

 Alexandra Gheorghiu ,  Cosmin Ungureanu

Alexandru Ioan Cuza University of Iasi, Romania


**Abstract:** This study analyses the European Union's regulatory frameworks on data protection and consumer rights. It examines landmark legislations such as the General Data Protection Regulation (GDPR), the Data Governance Act (DGA), and others that shape data privacy, digital content management, and consumer protection across the EU. Utilizing Iramuteq software for content analysis, it identifies thematic clusters and relationships within the texts, uncovering core concepts like digital service conformity, consumer rights, and the role of public data governance. Through cluster and factor analysis, the study reveals how these legal instruments collectively promote data security, innovation, and market fairness while ensuring consistent consumer protection and legal compliance throughout EU member states.

**Keywords:** EU Directives, GDPR, data protection, consumer rights, digital economy

## Introduction

The European Union has established a comprehensive regulatory framework to manage the complexities of data governance and digital services in the modern era. This framework fosters innovation while protecting consumer rights and ensuring data privacy, striking a careful balance between technological progress and strong personal data safeguards. Key regulations like the General Data Protection Regulation (GDPR) and the Data Governance Act (DGA) set international benchmarks for responsible data usage and transparency, promoting economic growth alongside ethical governance. These regulations serve as the foundation of the EU's approach to personal data protection, digital services, and market equity. This following analysis will explore the various legislative measures put in place by the EU to regulate the digital economy by examining how directives and regulations interact with one another to create a coherent legal framework that addresses the diverse challenges of digital transformation. The analysis was performed using the software Iramuteq. Iramuteq is an open-source software that specializes in textual data analysis, allowing researchers to explore bodies of text using a variety of statistical methods, including cluster analysis, correspondence analysis, and factor

---

 Centre for European Studies, Faculty of Law, Alexandru Ioan Cuza University of Iasi, Romania; e-mail: gheorghiu.anda@yahoo.com.

analysis. The software's capabilities make it particularly effective for identifying patterns, relationships, and themes within complex texts. The first methodological step involved importing the texts of the selected EU directives and regulations (separately) into Iramuteq, which processed the data to identify word frequencies and co-occurrences. This initial analysis provided a foundation for the subsequent cluster analysis, where Iramuteq grouped words and phrases that frequently appeared together into distinct clusters. These clusters revealed significant thematic connections, such as those related to consumer protection, digital content, and data privacy. The software's ability to display the clusters visually allowed for an interpretation of the relationships between terms. Finally, following the cluster analysis, a factor analysis was conducted using Iramuteq to reduce the complexity of the text data and identify underlying dimensions that structure the corpus of directives and regulations.

## 2. Directive analysis

The subsequent analysis relies on several directives and regulations linked to data, database creation, and data protection. Four directives were selected for this analysis: Directive 96/9/EC (Directive 96/9/EC on the legal protection of databases, n.d.) of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Directive (EU) 2019/770 (Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, n.d.) of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Directive (EU) 2019/771 (Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, n.d.) of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC (Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, n.d.)<sup>1</sup>, and repealing Directive 1999/44/EC, and Directive (EU) 2019/1024 (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, n.d.) of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Using these directives allows for a comprehensive approach to consumer protection (Directive (EU) 2019/770,

---

<sup>1</sup> Directive 2009/22/EC was replaced by Directive 2020/1828, however, at the time of the analysis, the corpus of the Directive 2009/22/EC was used

Directive (EU) 2019/771, and Directive (EU) 2019/1024) and data regulation (Directive 96/9/EC) in the EU. This multifaceted approach establishes a robust regulatory framework that promotes data integrity, consumer protection, innovation, and economic growth.

Directive 96/9/EC (Directive 96/9/EC on the legal protection of databases, n.d.) of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, establishes the legal framework for the protection of databases within the European Union. It defines a database as a collection of independent works, data, or materials systematically or methodically arranged and individually accessible by electronic or other means. The directive specifies that its protection does not extend to computer programs used in creating or operating databases but focuses instead on the database itself. The directive details two main types of protection: copyright protection for databases that constitute an author's own intellectual creation due to the selection or arrangement of their contents, and a sui generis right for databases that demonstrate a substantial investment in obtaining, verifying, or presenting contents. Copyright protection does not cover the data itself but the structure, selection, or arrangement of the database. Conversely, the sui generis right protects against unauthorized extraction and re-utilization of substantial parts of the database, regardless of the originality of its contents. The rights under the directive include control over reproduction, distribution, and public display of the database. Exceptions to these rights are allowed for specific purposes such as private use, teaching, public security, and certain judicial and administrative procedures, provided these do not unreasonably prejudice the legitimate interests of the rights holder. This ensures that while database makers enjoy a robust level of protection, users also retain certain freedoms to access and use the data for legitimate purposes. The directive also mandates that member states must provide appropriate legal remedies for any infringement of these rights and requires regular reviews to ensure the directive's application does not lead to market abuses or hinder competition.

Directive (EU) 2019/770 (Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, n.d.) of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, aims to ensure a high level of consumer protection and the smooth functioning of the internal market concerning contracts for the supply of digital content and digital services. It sets out common rules on the conformity of digital content or services with contracts, remedies for non-conformity or non-supply, and the conditions under which digital content or services can be modified. This directive encompasses various forms of digital content and services, including those allowing consumers to interact with data or integrate digital solutions into their own digital environments. The directive outlines specific definitions crucial for its application, such as 'digital content',

'digital service', and 'goods with digital elements'. It applies to any contract where a trader provides digital content or services in exchange for a price or personal data, except under specified exemptions such as healthcare and gambling services. It also details scenarios where digital content is integrated into consumer's digital environments, emphasizing compatibility, functionality, and interoperability requirements. In terms of consumer rights and trader obligations, the directive ensures that digital content and services conform to the contract at the time of supply and throughout their duration if meant to be supplied over time. Consumers are entitled to remedies such as repair, replacement, or price reduction if the digital content or services fail to meet contractual standards. Moreover, the directive stipulates conditions under which the consumer can terminate the contract, especially if the trader fails to supply the digital content or service or if there is a lack of conformity after a trader's attempt to rectify it. Finally, the directive places a significant emphasis on ensuring continuous conformity by requiring traders to provide necessary updates, including security updates. It also allows for modifications to digital content or services provided they are justified, do not incur additional costs, and are communicated clearly to the consumer. The directive stresses that any contractual terms disadvantaging the consumer compared to the protections offered by the directive are not binding. It sets a framework for the transposition of these provisions into national law by July 1, 2021, with application starting from January 1, 2022.

Directive (EU) 2019/771 (Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, n.d.) of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, focuses on enhancing consumer protection and ensuring the smooth functioning of the internal market through uniform rules on sales contracts. This directive replaces Directive 1999/44/EC and amends Regulation (EU) 2017/2394 and Directive 2009/22/EC. Its primary objective is to standardize the obligations and rights in sales contracts between consumers and sellers, specifically addressing the conformity of goods, available remedies for non-conformity, the exercise of these remedies, and the conditions surrounding commercial guarantees. The definitions set forth in the directive provide clarity on various terms such as "consumer", "seller", "goods", and "digital content", setting the scope for its application. It applies to all sales contracts where a consumer purchases goods from a seller for non-commercial purposes. The directive emphasizes that goods must meet specified contractual and objective standards at the time of delivery, including expected functionality, compatibility, and durability. It also specifically addresses goods with digital elements, acknowledging the increasing integration of digital technology in consumer goods. The directive

outlines the remedies available to consumers when purchased goods do not conform to the contract. These include the right to repair or replacement, a price reduction, or contract termination, under certain conditions. The seller is liable for any lack of conformity that becomes apparent within two years of delivery. For goods with digital elements, the directive mandates that sellers provide necessary updates to maintain conformity, highlighting the evolving nature of consumer products and the importance of ongoing support.

Directive (EU) 2019/1024 (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, n.d.) of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, aims to advance the utilization of open data and bolster the innovation of products and services by setting minimum rules for the reuse of public sector information. This encompasses documents held by public sector bodies and public undertakings across the Member States, as well as certain research data under specified conditions. The directive explicitly excludes documents outside the public sector bodies' defined tasks, those for which third parties hold intellectual property rights, and sensitive data among others, ensuring that the reuse aligns with legal frameworks and respects private and sensitive information. Key definitions provided within the directive clarify terms such as "public sector body", "document", "research data", and "high-value datasets", which are essential for understanding the scope and application of the regulations. These definitions are critical for categorizing and standardizing the data that the directive covers, ensuring clarity and uniformity in the data available for reuse. The directive promotes the concept of "open by design and by default", encouraging public sector bodies to make documents accessible in open, machine-readable formats wherever possible. The directive establishes that, generally, the reuse of documents should be free of charge, but allows for the recovery of marginal costs related to the reproduction and dissemination of documents. It provides exceptions for public sector bodies that need to generate revenue to cover substantial parts of their costs, thus balancing public access to information with the financial sustainability of public services. Moreover, the directive encourages transparency in setting and calculating any charges for reuse, requiring public sector bodies to publish these details openly. Finally, Directive (EU) 2019/1024 mandates Member States to facilitate access to documents through various technical and administrative arrangements, including the development of asset lists and digital portals to enhance document discoverability. By July 2021, Member States are required to adopt all measures necessary to comply with the directive, ensuring that national laws align with its provisions. The directive also emphasizes the need for regular reviews and updates to adapt to technological and market changes, highlighting the dynamic nature of public data and its potential to drive innovation and economic growth within the EU.

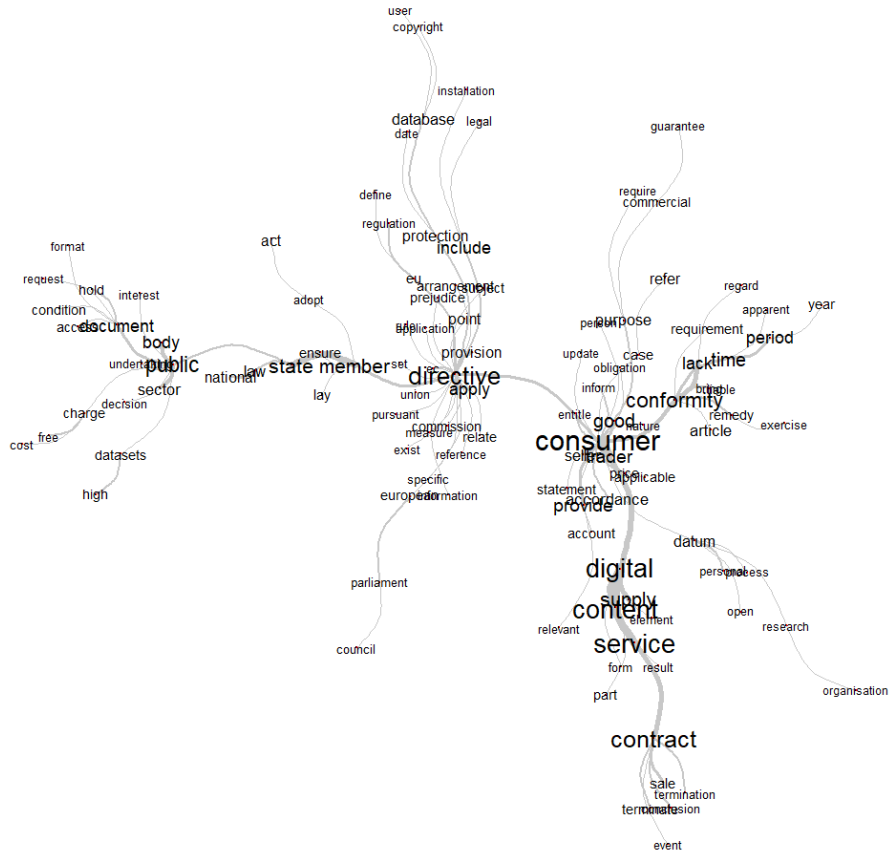
As seen in Figure 1, several key word clusters have emerged by analyzing the four directives together. The "consumer" cluster seems extremely closely knit to words such as "conformity", "good", "trader", "applicable", but also with "digital", "content", "service" and "supply". These terms suggest that consumers have specific rights and the ability to exercise those rights under the contracts agreed upon with digital service providers. This reinforces the idea that EU legislation not only sets standards but also empowers consumers to actively ensure those standards are met, providing mechanisms for recourse in cases where digital services fail to comply with contractual obligations. The subsequent cluster leads with "European Union", "state member", "directive", "apply", "national", "law" and "provision." These terms emphasize the detailed legal mechanisms through which directives are transposed into national legislation. The Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, n.d.) is transposed in Romania through the law on copyright and related rights (Official publication: *Monitorul Oficial al României* ; Number: 60 ; Publication date: 1996-03-26 ; Page: 00002-00021), the law amending and supplementing law no. 8/1996 on copyright and related rights (Official publication: *Monitorul Oficial al României* ; Number: 587 ; Publication date: 2004-06-30 ; Page: 00001-00024), the emergency government ordinance amending and supplementing law no. 8/1996 on copyright and related rights (Official publication: *Monitorul Oficial al României* ; Number: 843 ; Publication date: 2005-09-19 ; Page: 00001-00016) , and the law approving government emergency ordinance no. 123/2005 amending and supplementing law no. 8/1996 on copyright and related rights (Official publication: *Monitorul Oficial al României* ; Number: 657 ; Publication date: 2006-07-31 ; Page: 00002-00012). The Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services translated into Romanian national legislation through Government emergency ordinance no. 141/2021 on certain aspects relating to contracts for the supply of digital content and digital services (Official publication: *Monitorul Oficial al României* ; Number: 1248 ; Publication date: 2021-12-30) as well as the Government decision no. 372/2022 amending and supplementing the annex to Government decision no. 1.553/2004 on certain methods for terminating unlawful practices in the field of protection of collective consumer interests and the annex to Government decision no. 444/2020 on establishing the institutional framework and certain measures for implementing the provisions of article 5(1) of Regulation (EU) 2017/2,394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for enforcing consumer protection laws and repealing Regulation (EC) No. 2.006/2004 (Official publication: *Monitorul Oficial al României* ; Number: 276 ; Publication date: 2022-03-22 ; Page: 13). Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain

aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC was transposed in the national legislation in the Government emergency ordinance no. 140/2021 on certain aspects relating to contracts for the sale of goods (Official publication: *Monitorul Oficial al României* ; Number: 1245 ; Publication date: 2021-12-30) and the Government decision no. 372/2022 . Finally, the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information was translated nationally into the law no. 179 of June 9, 2022 on open data and the reuse of information from the public sector (Official publication: *Monitorul Oficial al României*; Number: 57; Publication date: 1001-01-01). “Law” refers to the actual legal statutes enacted by member states while “provision” can indicate specific clauses or requirements within the directives that must be implemented.

This highlights the structured approach to ensure that all provisions of EU directives are incorporated into national laws effectively and uniformly. The cluster “public”, “free”, and potentially “body” (inferred as “public body”) not only supports transparency and democratic engagement but also fosters an environment where public sector data can be utilized freely for educational, research, and other public interest projects. This approach encourages openness and the sharing of resources managed by public institutions, aligning with wider goals of government accountability and public empowerment.

Furthermore, the word “access” underscores the directive’s intention to ensure that the free flow of information from public bodies is not just available but also easily accessible to the public, facilitating greater engagement and utilization of public sector resources for various legitimate purposes. The words “database”, “legal”, and “protection” form a cluster that deals specifically with the legal aspects of database management within the EU. This cluster emphasizes the protection of the structure, organization, and accessibility of databases, ensuring that database creators receive recognition and safeguarding of their intellectual property, while also balancing these protections with provisions for lawful access and use under specific circumstances. The dual mention of “public” (once with respect to general access to information and again with databases) signifies the balance the EU strives to maintain between protecting intellectual property and promoting innovation and public knowledge.

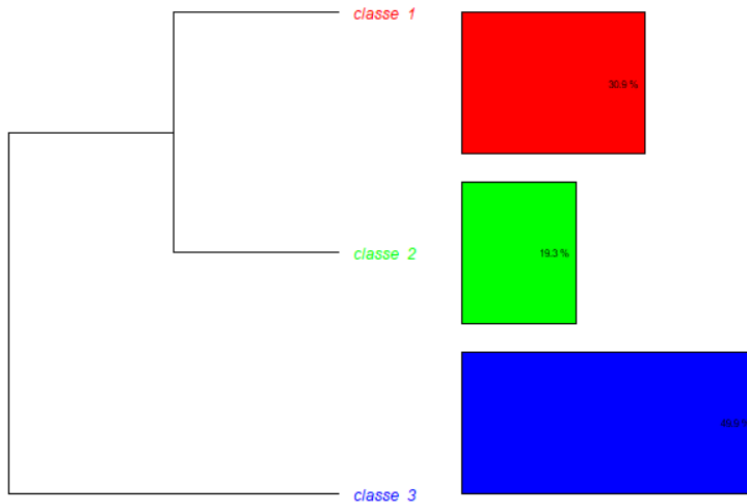
**Figure 1. Overall representation of the cluster analysis on EU directives regarding data**



Source: authors' representation

Following this analysis, we aimed to explore and determine whether these directives could be grouped into a specific factor structure. The factor analysis revealed the presence of three main factors.



**Figure 2. Factor structure for the directives on EU data regulation**

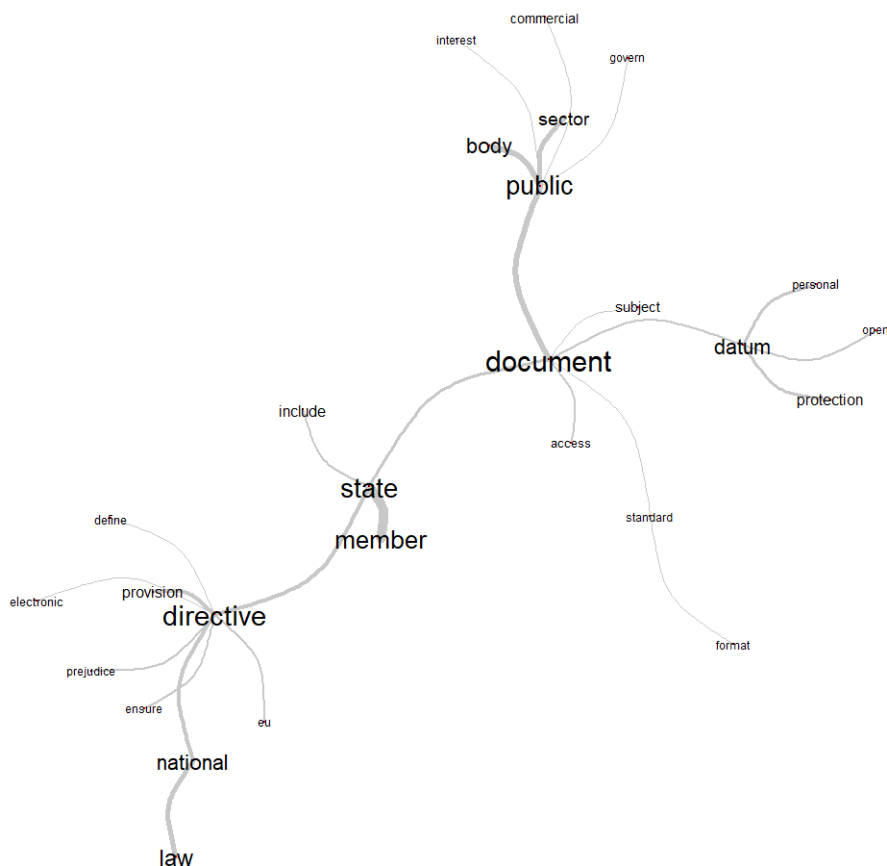
Source: authors' representation

The factor structure highlights three different classes. The first (30.9%) and the second one (19.3%) are grouped together, while the third one, and the one explaining most variance (49%), is separate. We will begin analysing each factor.

The first factor, explaining 30.9% of the whole variance, seems to regroup elements that are linked to law, directives, standards, and regulations. As seen in Figure 3, the terms “document”, “datum”, and “state member” are notably highlighted, suggesting a strong connection to the legislative texts and the mechanisms through which data and documents are regulated within the EU. Still central to the word cloud representing the first factor are the terms “directive” and “national”, pointing to the process of transposition where EU directives are incorporated into the national laws of member states. The presence of “law” connected directly to these terms underscores the binding nature of these directives upon member states, necessitating a harmonized approach across the EU to ensure consistency in legal standards, especially concerning consumer protection and digital transactions. Adjacent to these terms are “public”, “body”, and “protection”, which may refer to the public sector’s role in implementing these directives and the protection afforded to citizens and consumers under these laws. Lastly, the word “electronic” links back to the emphasis on digital solutions and the electronic management of data across sectors, which is a key aspect of the modernized approach the EU takes towards digital content and services. This reflects an evolving legislative landscape that accommodates the rapid growth of digital technologies, aiming to protect personal data and regulate the digital market effectively. The cluster of terms in the word cloud effectively maps out the interconnected nature of

EU directives, national laws, public administration, and the overarching goals of data protection and accessibility within the European Union.

**Figure 3. First factor extracted from the EU Directives**

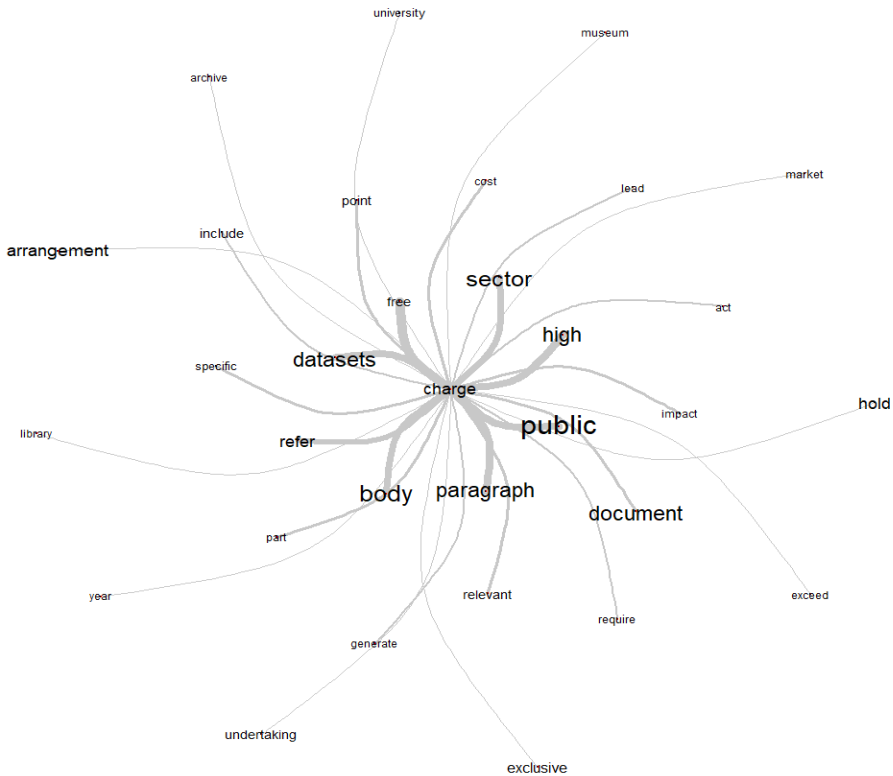


Source: authors' representation

The second factor extracted by the analysis can be visualized in Figure 4. Compared to the first factor, which primarily dealt with the legal frameworks and governance structure set by various EU directives, this second factor is more focused on the practical implications of these policies, specifically in terms of data management and accessibility within the public sector. The emphasis here is less on the legal mechanics and more on the operationalization of these laws through the standardization and dissemination of public sector information. This shift from legal structure to practical application highlights the directive's role in shaping how public

data is effectively managed and utilized, aiming to foster an environment where public sector information supports innovation, governance, and public engagement within the EU. Central to the visualization are terms like “datasets”, “public”, “sector”, “body”, and “document”, which underscore the directive’s focus on structuring public data in a way that facilitates broader access and utility. This directive aims to standardize how data is shared across different platforms within the public domain, making it available to various stakeholders, including educational and cultural institutions like universities, museums, archives, and libraries. These institutions are explicitly recognized as key holders of significant public datasets. The directive encourages these bodies to provide public access to their collections, thereby supporting educational, cultural, and research activities. In terms of economic implications, the words “free”, “charge”, and “cost” reflect the directive’s stipulations on the financial aspects of data access.

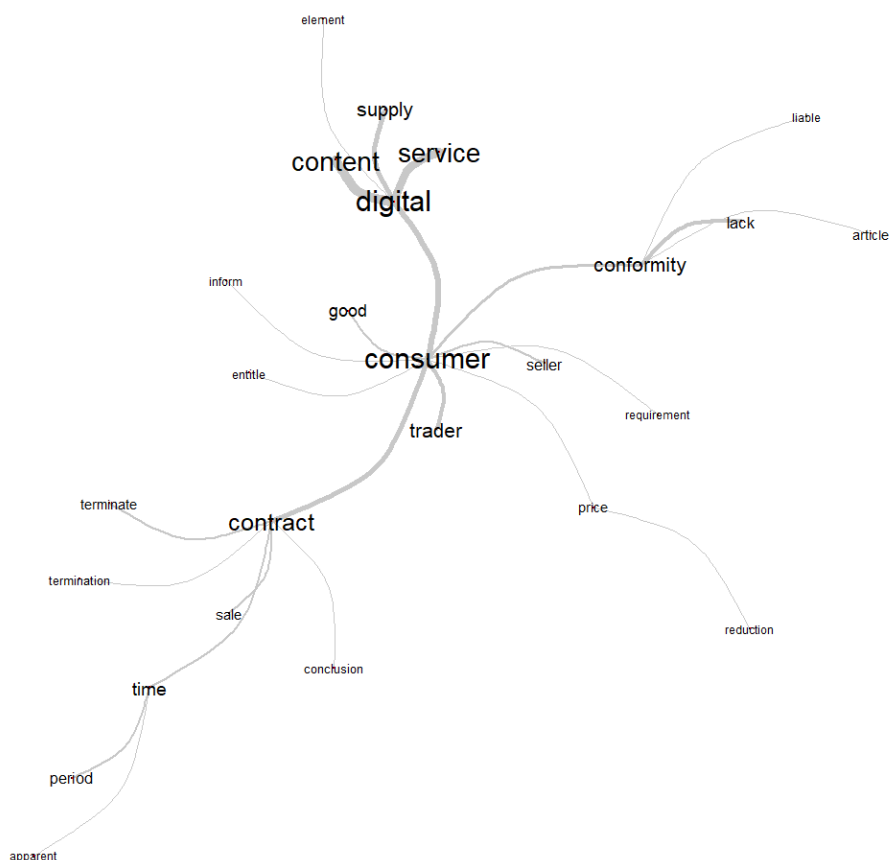
**Figure 4. Second factor extracted from the EU Directives**



Source: authors’ representation

The structure of the final factor can be analysed in Figure 5.

**Figure 5. Third factor extracted from EU Directives**



Source: authors' representation

The third factor extracted from the directives focuses on the contractual relationships and obligations between consumers, traders, and digital content or service providers, as evident from the central terms in the word cloud like “consumer”, “contract”, “trader”, “digital”, “service”, and “content.” This factor emphasizes the specific aspects of consumer rights, trader obligations, and the conformity of services and goods within digital transactions. These directives establish guidelines on the conformity of digital services and goods, the contractual standards between consumers and traders, and remedies available in instances of

non-conformity. Unlike the first factor, which primarily outlined the legislative and regulatory frameworks governing data protection and public sector information management, and the second factor, which focused on the accessibility and economic considerations of public sector datasets, this third factor delves into the dynamics of marketplace transactions specifically within the digital realm. It underscores how contractual terms are defined and enforced in the context of digital services and goods, highlighting the interactions between “consumer”, “trader”, and “digital content”. Key terms like “conformity”, “lack”, “requirement”, and “supply” point directly to the obligations of traders to meet specified standards of service quality and information as mandated by the EU directives. These include ensuring that digital content and services supplied to consumers conform to the agreed contractual descriptions and functionalities. The focus on “contract” and “termination” reflects the rights of consumers to terminate contracts under certain conditions, such as failure to comply with the terms or correct issues of non-conformity, which are stipulated under these directives. The word cloud also highlights terms such as “good”, “price”, and “reduction”, which connect to the economic aspects of consumer transactions in the digital market. These terms suggest the consideration of pricing transparency and the potential financial remedies like price reductions when digital goods or services fail to meet contractual expectations.

### **3. Regulations analysis**

The European Union has developed a robust regulatory framework to govern various aspects of data privacy, security, and digital markets. This framework is composed of several key regulations, each addressing specific sectors or challenges in the rapidly evolving digital landscape. Regulations such as the Data Governance Act, the Digital Markets Act, and the General Data Protection Regulation (GDPR), among others, play a critical role in shaping the legal environment for digital services, data use, and consumer protection within the EU. These regulations not only promote innovation and competitiveness but also ensure the protection of fundamental rights, particularly in relation to data privacy and security.

The Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, known as the Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, n.d.), establishes a comprehensive framework for data governance within the European Union. It focuses on conditions for the re-use of data held by public sector bodies, a supervisory framework for data intermediation services, and mechanisms for the registration of entities engaging in data altruism. Importantly, the regulation does not obligate public sector bodies to allow data re-use nor does it exempt them from confidentiality obligations under existing laws. This regulation is pivotal for

maintaining a balance between facilitating data access and ensuring compliance with data protection standards. The act also introduces the European data innovation board, enhancing collaboration and consistency across EU member states in data handling practices. This includes adherence to stringent data protection laws like GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and others that govern personal and non-personal data. The board's role underlines the EU's commitment to a unified approach in data governance, emphasizing the protection of personal data while fostering innovation and ensuring that data governance practices do not conflict with individual data rights. The Regulation (EU) 2022/868 is instrumental due to its integration with existing data protection frameworks and its emphasis on regulatory oversight. The act's provisions ensure that any processing of personal data within the governance framework respects the established privacy rights under EU law, making it a critical component in understanding the landscape of data privacy and security regulations in the EU.

The Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC, n.d.) could be used to examine how legislations that are not primarily focused on data protection still incorporate rigorous data privacy measures to comply with the EU's comprehensive privacy and data protection framework. This ensures that even regulations aimed at public safety and emergency response are designed in a way that respects and protects individual privacy rights. More specifically, regulation (EU) 2015/758, enacted by the European Parliament and Council on April 29, 2015, sets forth the type-approval requirements for the deployment of the 112-based eCall in-vehicle system across the European Union. This regulation mandates that all new types of vehicles, specifically categories M1 and N1 as defined in Directive 2007/46/EC, be equipped with the eCall system. This system is designed to enhance vehicular safety by ensuring that in the event of a severe accident, emergency services are automatically notified through the eCall system which uses the pan-European emergency number, 112. The eCall system can be triggered automatically by in-vehicle sensors during an accident or manually by vehicle occupants, thereby facilitating rapid response times from emergency services, potentially saving lives and reducing injury severity. A significant emphasis is placed on privacy and data protection within the framework of the eCall system. The regulation aligns with existing EU data protection directives to ensure that any personal data transmitted during emergencies is strictly used for the purpose of emergency handling. Manufacturers must incorporate privacy-enhancing

technologies to safeguard user data and prevent unauthorized tracking. The eCall system is designed to store only essential data temporarily, ensuring that data retention does not exceed the necessary duration for emergency response. These provisions underscore the EU's commitment to respecting individual privacy while leveraging technology to enhance public safety on roadways.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, n.d.), is designed to ensure fair and contestable markets within the digital sector across the European Union, particularly focusing on entities designated as "gatekeepers." These gatekeepers are large platforms that control core platform services, such as social networks, search engines, and online intermediation services, which are crucial gateways for businesses to reach consumers. The regulation aims to prevent these gatekeepers from exploiting their powerful market positions by setting out specific rules that ensure they engage in fair and open practices. The digital markets act introduces several key obligations for gatekeepers, such as prohibiting them from combining personal data across services without explicit consent, ensuring interoperability of services, and providing business users with access to their data. These measures are intended to increase competition and innovation by preventing gatekeepers from enforcing restrictive conditions that could disadvantage other market participants. Additionally, gatekeepers are required to notify the European Commission of certain mergers and acquisitions, which allows the Commission to assess the potential impact of such market consolidations on competition. In the context of data privacy and security, the digital markets act complements the general data protection regulation (GDPR) by addressing the specific challenges posed by the digital economy's scale and scope. The DMA regulates the processing of personal data beyond the GDPR's requirements by imposing additional controls on gatekeepers, such as limiting data combination and enhancing user consent protocols. This focus ensures that the expansive control of digital platforms does not undermine user privacy and encourages a more equitable digital market landscape. The regulation's provisions for data handling and platform interoperability make it a significant instrument in the broader analysis of EU data protection, privacy laws, and digital regulation, ensuring that major platform operators cannot bypass EU-wide protections afforded to individuals and businesses.

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

of personal data and on the free movement of such data, and repealing Directive 95/46/EC, n.d.), known as the General Data Protection Regulation (GDPR), is a comprehensive data protection regulation that establishes guidelines for the collection, storage, and processing of personal data within the European Union. The regulation is designed to strengthen and unify data protection for all individuals within the EU, ensuring that their fundamental rights and freedoms, particularly their right to the protection of personal data, are safeguarded. The GDPR applies to both automated personal data and manual filing systems, where personal data are accessible according to specific criteria. A core component of the GDPR is its expansive scope, applying not only to organizations based within the EU but also to those outside the EU that process data related to offering goods or services to, or monitoring the behaviour of, EU data subjects. This wide-reaching applicability makes the GDPR a critical element in global data protection frameworks, as it mandates compliance from virtually any significant digital operation interacting with EU residents. The regulation sets forth principles for data processing—such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality—which must be demonstrably adhered to by data controllers and processors. The GDPR serves as a foundational text. It not only outlines the conditions under which personal data may be processed and transferred but also details the rights of data subjects, including access to data, correction, deletion (the right to be forgotten), and the right to object to data processing. The GDPR's provisions for data protection impact assessments, data protection officers, and significant penalties for non-compliance underscore its role as a stringent and influential framework in shaping global data protection practices. This regulation is indispensable for understanding the complexities and requirements of modern data privacy and security law in Europe and serves as a model for similar laws worldwide.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, n.d.) enacted on November 14, 2018, establishes a framework to ensure the free flow of non-personal data within the European Union. This regulation is crucial as it addresses data localization requirements, aiming to prohibit restrictions imposed by member states that mandate data storage and processing within their territories unless justified by public security. It is designed to bolster the data economy by making non-personal data more accessible and usable across the EU, which is pivotal for enhancing competitiveness and innovation within the single market. A key aspect of this regulation is the facilitation of data availability for professional users and the competencies of authorities to access data for regulatory or official duties. It mandates that any access restrictions cannot be based on where data is stored or processed within the EU, ensuring that businesses and



services operate more fluidly across national borders. This is particularly relevant in a digital single market, as it supports a cohesive digital economy, reduces operational hindrances, and increases efficiency. The regulation is also significant in the context of comprehensive data regulation within the EU, particularly in relation to the General Data Protection Regulation (GDPR), which governs personal data. Regulation (EU) 2018/1807 clarifies procedures for data sets composed of both personal and non-personal data, ensuring that the free flow of non-personal data does not compromise personal data protection standards. This dual-framework strengthens the overall data governance within the EU, making Regulation 2018/1807 a critical component in the analysis of EU-wide data privacy, security, and regulatory practices, enhancing the understanding of how non-personal and personal data interact within the regulatory landscape.

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 (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, n.d.), commonly referred to as the Digital Services Act, sets out a comprehensive framework aimed at ensuring a safe, predictable, and trusted online environment within the EU's digital single market. This regulation specifically targets intermediary services, focusing on harmonizing rules across the EU to enhance consumer protection and uphold fundamental rights. One of the regulation's key features is the conditional exemption from liability for providers of intermediary services, paired with specific due diligence obligations tailored to certain categories of providers. This framework aims to balance the facilitation of innovation and business activities online with stringent consumer protection and privacy standards. The digital services act's scope includes all intermediary services provided in the EU, regardless of the provider's location, ensuring that even non-EU based companies must comply when serving EU residents. This broad applicability signifies a major step towards regulating the digital space effectively across international borders, addressing issues such as illegal content, transparency, and fairness in digital services. Importantly, the regulation details mechanisms for cooperation and coordination among EU member states, ensuring that enforcement is uniform and effective across the single market. The digital services act complements existing regulations like the GDPR by reinforcing the responsibilities of digital service providers in protecting user data and promoting transparency. The regulation mandates clear terms and conditions, outlines processes for content moderation, and establishes robust measures against illegal content, all while emphasizing the need for respecting user privacy and providing clear mechanisms for redress and compliance. For scholars and policymakers analyzing main regulations on data privacy and security, the digital services act offers a pivotal case study on the EU's approach to modernizing and securing the digital market in alignment with its fundamental rights and values.

**Figure 6. Graph Analysis on EU Regulations regarding data**



Source: authors' representation

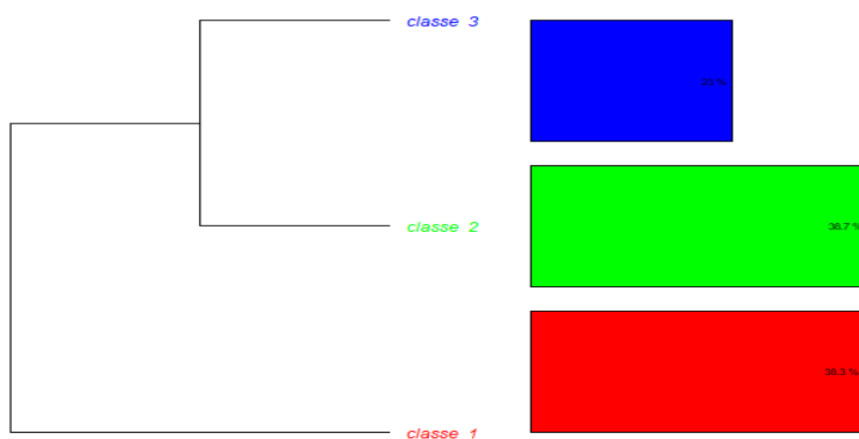
The ensemble of EU regulations discussed provides a comprehensive overview of the European Union's systematic approach to digitalization, highlighting a deep commitment to both innovation and the safeguarding of fundamental rights. These regulations collectively address the multifaceted aspects of digital transformation within the EU, from ensuring personal and non-personal data flow freely and securely across member states to establishing a secure digital environment for consumers and businesses alike. For instance, the General Data Protection Regulation (GDPR, Regulation 2016/679) sets a benchmark globally for the protection of personal data, ensuring data privacy remains a priority amidst the digital economy's expansion. Similarly, the Free Flow of Non-Personal Data Regulation (2018/1807) complements the GDPR by facilitating the unrestricted movement of non-personal

data, thus fostering a competitive data economy and innovation. Moreover, the introduction of sector-specific regulations like the eCall Regulation (2015/758) and the Digital Markets Act (2022/1925) reflects the EU's tailored approach to addressing unique challenges within different digital sectors. The eCall Regulation enhances safety through digital technologies, mandating all new vehicles to be equipped with an automatic emergency call system, while the Digital Markets Act targets large online platforms to ensure they operate fairly, promoting contestable and fair digital markets. The Data Governance Act (2022/868) further supports this ecosystem by setting out measures to enhance trust in data sharing and the re-use of public sector information, crucial for AI and machine learning advancements. The comprehensive nature of these regulations ensures that the EU not only adapts to digital advancements but also proactively shapes the digital landscape to reflect its core values of fairness, safety, and respect for individual rights.

As seen in Figure 6, the centrality of “datum/data” underscores the core importance of data in the digital economy within the EU legislative framework. This highlights the EU's focus on data as a crucial asset that drives not only economic activities but also impacts consumer protection, privacy, and digital services. The surrounding terms such as “provider”, “trader”, and “platform” suggest a focus on entities that handle, process, or utilize data in their operations. The network suggests a structured approach to understanding how regulations influence member states and the entities operating within them, reflecting the governance and compliance mechanisms set by the EU. Providers of digital content and services are under stringent obligations to ensure that their offerings meet the specified criteria for quality, safety, and consumer rights protection as laid out in the regulations. This encompasses not only the provision but also aspects like the right of consumers to receive updates and how these services integrate into the wider digital environment of the user, addressing interoperability and compatibility. Looking at the surrounding terms such as “regulation”, “compliance”, and “monitor”, the map encapsulates the legislative lifecycle—from the creation of regulations at the EU level to the practical aspects of compliance by affected entities. This highlights a multi-layered governance approach where EU regulations set the framework and are directly applicable across member states, ensuring uniformity in application. The presence of terms like “enforcement” underscores the role of national regulatory bodies in ensuring that the regulations' stipulations are met and maintained. Another significant aspect evident from the map is the emphasis on consumer rights and protections, particularly in the context of digital transactions and data usage. Terms like “consumer”, “user”, and “rights” reflect the EU's strong focus on protecting consumer interests in the digital age. This is particularly relevant in regulations that outline how consumers should be treated in terms of contract conformity, what remedies are available in cases of non-conformity, and how consumers' data must be handled by providers.

By using a factor analysis on the directives presented above, we were able to identify a factor structure that is represented below (Figure 7). The factor structure explains 93% of variance and has three main factors.

**Figure 7 – Factor analysis structure of EU Regulations regarding data**

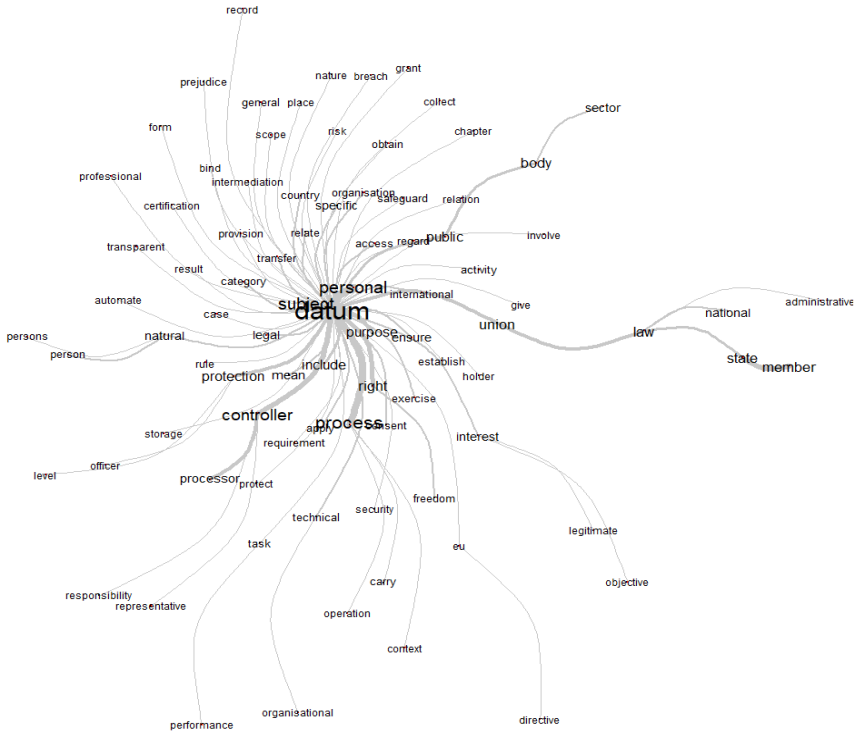


Source: authors' representation

The first factor explains 38.3% of the variance and revolves around “personal data”, reported here as “datum.” The word cloud reveals a dense network of terms that highlights key concepts in data protection, digital content, and consumer rights within the EU legislative framework. Central to this network is “datum”, surrounded by terms like “personal”, “subject”, “process”, and “controller”, which signify the foundational elements of data protection laws. This arrangement underscores the emphasis on personal data, indicating how it should be processed, the roles of data controllers (entities that determine the purposes and means of processing personal data), and the rights of data subjects (individuals whose personal data is processed). Surrounding these central terms are clusters that include “legal”, “protection”, “right”, “requirement”, and “security.” These terms connect closely with the legislative intent to safeguard personal data, ensuring that data processing adheres to legal standards that protect individual rights. The presence of “security” highlights the requirement for technical and organizational measures to protect data against unauthorized or unlawful processing, accidental loss, destruction, or damage. This reflects the regulations’ focus on not just the legality of data handling but also the practical aspects of data security and integrity. Another prominent cluster features terms like “national”, “member”, “state”, “law”, and “public.” These terms suggest the interaction between EU-wide regulations and national laws, highlighting the role of member states in implementing and enforcing EU regulations within their own legal frameworks. The reference to “public” and “state” indicates the involvement

of state bodies in the administration of these laws, which could include public access to information, state oversight of data protection practices, and the handling of data in public sector operations.

**Figure 8. First factor extracted from the EU regulations regarding data**



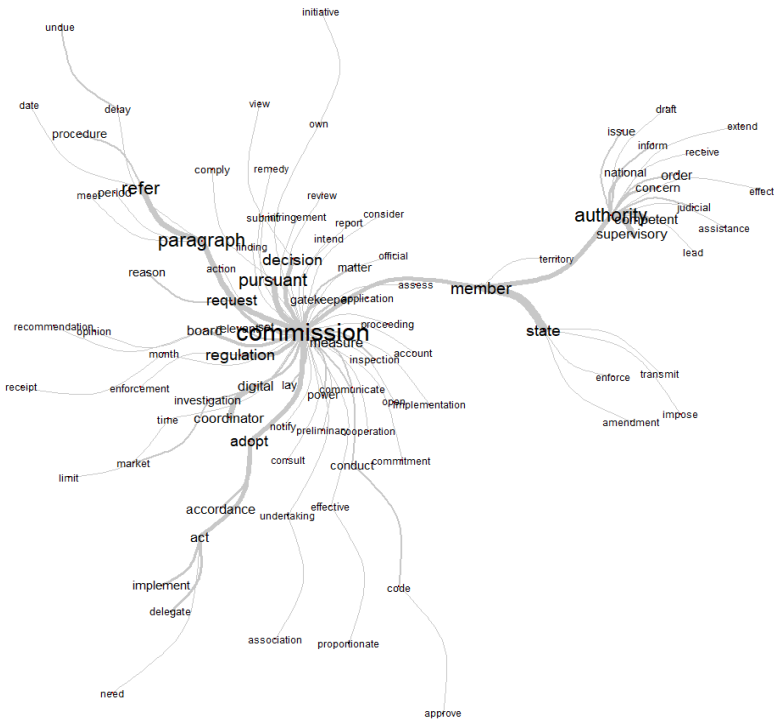
Source: authors’ representation

Lastly, terms like “directive”, “EU”, “international”, “union”, and “administrative” reflect the broader context in which these regulations operate. The use of “directive” points to the form of legislation that requires member states to achieve a particular result without dictating the means of achieving that result. This network of terms paints a comprehensive picture of the EU’s legislative approach, emphasizing data protection as a pivotal aspect of the digital single market, shaped by a complex interplay of legal, security, and administrative considerations.

The second factor that was extracted explains 38.71% of variance and is mainly focused on legislative actions, such as adoption, procedures, etc. Figure 9 highlights the main connections between the terms associated with factor 2. The word cloud appears to focus heavily on the procedural and regulatory aspects of EU legislation, particularly highlighting the roles and processes that govern the implementation and enforcement of regulations. Central to the diagram are the terms

“Commission”, “regulation”, and “adopt”, which together suggest a primary focus on the European Commission’s role in developing and formalizing regulations that are then adopted across member states. This process underscores the European Commission’s pivotal role in initiating legislative actions that are aimed at harmonizing practices across the EU, maintaining oversight, and ensuring that the regulations are effective and proportionate to the goals they aim to achieve.

**Figure 9. Second factor extracted from the EU regulations regarding data**



Source: authors’ representation

Around these central terms, other significant terms like “member”, “state”, “authority”, and “national” reflect the multi-layered governance structure of the EU, where directives from the Commission must be transposed into national laws by member states. This transposition process requires member states to not only adopt the EU-wide regulations but also tailor their application to fit within their own legal frameworks and administrative practices. The terms “enforce” and “implementation” nearby further suggest the necessary actions taken by national authorities to ensure that these directives are applied effectively within their



services, emphasizing interactions among providers, consumers, and the regulatory frameworks governing these relationships. At the heart of the cloud (Figure 10), terms like “service”, “provider”, “platform”, and “online” are prominently featured, highlighting the focus on digital service platforms—entities that offer various online services to consumers. This includes everything from cloud services to social media platforms, reflecting the broad scope of the EU’s digital market regulations. Surrounding these central terms are “search”, “engine”, and “large”, which may refer to the major search engines and large online platforms that dominate the market. This points towards regulatory interests in how these platforms operate and interact with both users and smaller businesses, ensuring they engage in fair practices and comply with EU data protection and consumer rights laws. The presence of “audit”, “compliance”, and “contract” suggests mechanisms through which these regulations are enforced, indicating that platforms must adhere to specific standards and are subject to periodic reviews and audits to ensure their operations remain within legal bounds. Additionally, the word cloud includes terms like “consumer”, “trader”, and “intermediary”, which delineate the different roles within the digital economy. Consumers are the end-users of services, traders could be businesses utilizing platforms to reach consumers, and intermediaries might be the platforms themselves or third-party services that facilitate transactions or content delivery. This tripartite relationship underscores the complex interactions that EU directives aim to regulate, focusing on transparency, fairness, and data security within these engagements.

These regulations aim to foster a balanced ecosystem in which technological advancement and innovation can progress within a framework that considers human rights, privacy, and ethical standards. The EU’s legislative environment could potentially serve as a model for other regions, illustrating how thoughtful regulation might support the digital economy while safeguarding individual and collective interests. This comprehensive approach is important for any in-depth analysis of laws regarding digitalization in the EU, suggesting ways in which laws might evolve to meet technological challenges while striving to ensure the security, privacy, and well-being of all stakeholders in the digital domain.

## **Conclusion**

In conclusion, the factor analysis of both the directives and regulations revealed some overlapping themes but it also highlighted distinct differences in their focus areas. In the directives, a key emphasis is placed on the harmonization of legal frameworks across member states, particularly concerning consumer protection and the operationalization of data governance within the public sector. Similarly, the regulations analysis emphasizes data protection and privacy as a central concern. However, while the directives focus more on the foundational legal structures and their implementation, the regulations analysis gives significant weight to the operational details of compliance, including how digital platforms and service



providers must adhere to strict rules governing data use and consumer interactions. Both analyses converge on the importance of consumer protection and data security, but the directives tend to focus on structuring frameworks and defining rights, whereas the regulations concentrate more on enforcement, compliance, and the operational mechanisms necessary to protect those rights in the digital marketplace.

**Acknowledgement:** This work was supported by a grant of the Ministry of Research, Innovation and Digitization, CNCS – UEFISCDI, project number PN-III-P4-PCE-2021-1878, within PNCDI III “Institutions, digitalization and regional development in the European Union”. The authors want to express their gratitude for the comments and guidance provided by professor Carmen Tamara Ungureanu with respect to the relevant directives and regulations.

## References

- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. (n.d.). <https://eur-lex.europa.eu/eli/dir/2019/1024/oj>
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. (n.d.). <https://eur-lex.europa.eu/eli/dir/2019/1024/oj>
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019L0770>
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019L0770>
- Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. (n.d.). <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32019L0771>
- Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC. (n.d.). <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32019L0771>
- Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. (n.d.). <https://eur-lex.europa.eu/eli/dir/2020/1828/oj>

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L1828&qid=1730728253078

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:31996L0009>

Directive 96/9/EC on the legal protection of databases. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31996L0009>

Directive 96/9/EC on the legal protection of databases. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:126028>

Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0758>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (n.d.). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. (n.d.). <https://eur-lex.europa.eu/eli/reg/2018/1807/oj>

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828. (n.d.). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925>

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. (n.d.). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724. (n.d.). <https://eur-lex.europa.eu/eli/reg/2022/868/oj>