EÖTVÖS LORÁND UNIVERSITY FACULTY OF LAW
DOCTORAL SCHOOLE

Boros Anita

THE LEGAL AND BUSINESS CHALLENGES OF DATA PROTECTION COMPLIANCE

PHD DISSERTATION
THESES

Supervisors:

Dr. Balogh Zsolt György **Dr. Faludi Gábor**

Budapest,
2025

1. Summary of the research task

Data protection law represents a highly dynamic and evolving field of legal concern, perpetually testing the limits of legislative capacity to keep pace. In the 21st century, digital transformation is inevitable; a greater proportion of business and personal lives are moving into the digital sphere. The majority of nascent enterprises operate without physical premises, and within this context, data is considered to be knowledge, and knowledge is power. As the British mathematician Clive Humby asserted in 2006, "data is the new oil"[1] signifying that information has become one of the most crucial resources. Indeed, it is an irrefutable fact that the value of data has now eclipsed that of oil. In the contemporary economic landscape, ensuring a sufficient level of data protection assumes paramount importance.[2]

Consequently, data asset management has emerged as a pivotal component of corporate strategies and innovations. It is evident that companies which proactively leverage the opportunities presented by big data, and which demonstrate superior capabilities in the areas of data utilization, storage, management, dissemination and protection, are able to secure a substantial competitive advantage.

Concurrently, the magnitude and repercussions of issues pertaining to private life are escalating. The European Union legal system has already imposed strict rules on the processing of personal data and defined sanctions against those who do not act lawfully during data processing. A growing number of cases have been brought before the European Court of Justice, thereby giving rise to conflicting decisions that are at odds with the right to privacy and the interests of businesses.[3] This finding is indicative of an emerging paradigm where the security of data is of paramount importance. However, technological development frequently outpaces legislative responses, creating a discrepancy between the pace of innovation and the regulatory framework.[4] Consequently, while the corporate sector expeditiously capitalises on the advantageous

---

[1] Nisha Talagala, Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,entity%20that%20drives%20profitable%20activity, Accessed: 12.10.2023.

[2] Jon Suarez -Davis, Data isn't 'the new oil' - it's way more valuable than that, https://www.thedrum.com/opinion/2022/12/12/data-isn-t-the-new-oil-it-s-way-more-valuable.

[3] T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, Data Protection: CJEU case law review – 1995-2020, https://www.dpcuria.eu/case-law-review-1995-2020.pdf, Accessed: 12.10.2023.

[4] Polyák Gábor, Szőke Gergely László: Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2704/1967, 31.p.

opportunities it proffers, individuals are bereft of the means to safeguard their privacy. The precise creation of data protection provisions and the delineation of sanctions were initially the purview of the member states, in consideration of the provisions of the European Union Data Protection Directive. Consequently, the digital market situation in Europe began to exhibit signs of distortion attributable to the absence of uniform regulation at the community level.

On 27 April 2016, the European Parliament and the Council adopted Regulation 2016/679 (Regulation on the protection of natural persons regarding the processing of personal data and on the free movement of such data), which replaced the Data Protection Directive 95/46/EC and all national legislation based on it.

The General Data Protection Regulation (GDPR) is a pertinent regulatory framework within this context, as it aims to establish a unified digital market and modernise the regulatory framework governing the processing of personal data, particularly regarding issues of security and citizen self-determination.

The present study is an academic response to the challenges arising from increasing data protection compliance obligations. It presents critical assessments of the domestic and international literature on data protection compliance and its impact on the business sphere.

While the principles of the GDPR apply equally to all organizations, the practical implementation of compliance can differ significantly between small and medium-sized enterprises (SMEs) and large companies. Nevertheless, given that SMEs account for 99% of businesses[5] in the European Union, the success of data protection regulation is largely reflected in the compliance level of SMEs.

The advent of the General Data Protection Regulation has led to the persistence of ambiguities surrounding data protection regulations. The enforcement of compliance with a unified regulatory framework is a complex undertaking, given the prevalence of general formulations within the regulation.

It is acknowledged that the level or extent of compliance with the regulation's rules may vary due to the specific geographical location or industry.

The objective of this study is to demonstrate that, for companies with limited resources and information management systems, data protection compliance entails significant work and a

[5] European Commision, Annual Report on European SMEs 2023/2024, Luxembourg: Publications Office of the European Union, 2024, 6.p.

considerable financial burden. This is because, in addition to complying with existing data management rules, it introduces new obligations for data controllers and processors that require the development of time-consuming and costly processes. One such example is the principle of accountability, which involves the transfer of responsibility from national authorities to organizations. This obliges the latter to demonstrate complete compliance with the legislation. This is a grave responsibility, especially for companies that handle large amounts of personal data, as compliance is not only a legal issue but also comprehensively affects process management, the control environment, and business processes. The challenges posed by the digital age extend to many areas, including but not limited to employee data management. This is a subject that already considers working from home, the use of personal devices, and online marketing. Furthermore, international trade and cooperation necessitate the transfer of personal data outside the European Union.

Considering prevailing data protection regulations, the research hypothesis can be postulated as follows: for a small or medium-sized company, it is impracticable to allocate sufficient time and resources to attain a high level of data protection compliance.

2. Methodological approach to the dissertation

To provide substantiation for the hypothesis, the present study presents critical assessments of the relevant national and international literature on compliance with data protection obligations and their impact on the business sphere. In addition to analyzing the guiding provisions of the General Data Protection Regulation, the discussion encompasses the positions, guidelines and recommendations of the Article 29 Working Party (WP29), the European Data Protection Board (EDPB) and various national data protection authorities, as well as the various compliance methods they have defined. Furthermore, an analysis of the fines imposed by several national authorities is conducted, with the objective of facilitating comprehension of the positions of data protection authorities and identifying the areas where data protection compliance is least successful.

The subsequent objective is to investigate the interpretation issues and shortcomings in the new data protection regulation. By comparing the legal issues that arise, a comprehensive picture of the consequences of the European uniform regulation will be created, and then the potential future problems in the field of data protection and the possible solutions that exist will be discussed.

The analysis of the issues determines the structure of the thesis and the methodology of the research, which includes a historical-descriptive and a descriptive-critical analysis.

Concurrently, the present study will be underpinned by a robust reliance on source analysis and secondary data analysis, with a primary focus on legal sources, international treaties, laws, regulations, the jurisprudence of judicial and other law enforcement bodies, and relevant legal literature. The objective of the research is to explore the drivers of our data protection rules and to understand the regularities. Rather than emphasizing generalizations, the focus will be on deriving specific findings from more general observations. After this, a summary of the characteristics of the cases drawn from the literature will be presented, and theoretical conclusions will be formulated.

The initial chapter of the thesis delves into the intricate relationship between the right to privacy and data protection. It then proceeds to offer a comprehensive overview of the repercussions of data protection regulation, meticulously enumerating both beneficial and detrimental outcomes. Subsequently, the thesis is divided into two substantial sections. In the initial section, an analysis is conducted of the obligations stipulated in the Data Protection Regulation. This analysis addresses any potential compliance difficulties and interpretation issues in relation to each obligation. In the second part of the thesis, the focus is on the practical challenges most frequently encountered during compliance.

Considering the rapid advancements and proliferation of artificial intelligence, it became imperative to undertake a comprehensive analysis of the associated data protection concerns within the thesis.

3. Outcome of the research and its possible applications

Conducting research in this area presents an opportunity to draw lessons that can provide real assistance to companies in complying with data protection regulations. Throughout the thesis, the objective is twofold: first, to explore the interpretation issues of the regulation, and secondly, to find answers to these issues.

Second, in addition to the discussion of legal requirements, I also formulate useful practical advice, which can serve as a basis for companies to develop their appropriate processes and information systems. In the practical challenges chapter, areas that affect most companies are analyzed, sinccomplyingtial step on the path to data protection compliance is to overcome the online

presence and the data protection challenges associated with data management, as well as to comply with data management in the workplace.

The central argument of this thesis is that the successful implementation of data protection compliance is an intricate undertaking. The data controller must demonstrate a commitment to continuous learning and adaptation, by maintaining a keen awareness of evolving interpretations and legal frameworks. This entails monitoring potential threats from both external and internal sources, ensuring adherence to existing organizational practices and regulations, and responding promptly to stakeholder inquiries. Above all, the role necessitates leadership skills that foster an appropriate organizational culture.

From the perspective of SMEs, the introduction of data protection regulations is often perceived as an additional task and obligation, as well as a cost and expense that may even result in a competitive disadvantage.[6]

The chapter on accountability shows that under the current regulation, accountability includes the most important task of the data controller, who must now not only take responsibility for complying with the principles and obligations set out in the regulation but must also be able to demonstrate compliance. Understanding the principle of accountability has become a cornerstone of effective data protection and a dominant trend in EU data protection law, policy, and organizational practice. Without compliance with this principle, we cannot talk about data protection compliance, which most companies forget about. After the GDPR comes into force, SMEs will have a significant problem in identifying to what extent the regulation applies to them, which data processing activities require special attention, and what documents they need to produce and processes they need to transform to demonstrate compliance.[7]

The chapters on impact assessment and data protection by default and by design demonstrate that, to comply with data protection regulations, the principles of data protection regulation must be incorporated into data processing technologies during both the design and operation phases. It is imperative that technology is designed and implemented in such a manner that its entire life cycle is compatible with the fundamental rights and values that define our democratic societies.

---

[6] According to a 2019 survey, 27 percent of European companies surveyed reported spending between €1,000 and €10,000 on data protection compliance, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/.

[7] Dr. Zemplenyi Adrienne: A KKV-k tapasztalatai a GDPR alkalmazásával kapcsolatban, STARII záró konferencia, https://naih.hu/files/dr-Zemplenyi-Adrienne_A-KKV-k-tapasztalatai-a-GDPR-alkalmazasaval-kapcsolatban_STARII-zarokonferencia.pdf, 1.p. Accessed: 12.12.2024.

However, it is important to note that conducting an impact assessment, such as the integration of data protection by design into the corporate culture, cannot be regarded as a standard obligation that can be fulfilled in a uniform manner across all companies. The onus, therefore, falls on data controllers to determine the application of suitable organizational and technical measures on a case-by-case basis. The determination of such measures may be contingent on factors such as the size of the organization, its target group, or even its core activity. Data protection by design is defined as a strategy that forms part of a long-term plan, which requires adherence to data protection principles and the rights and freedoms of data subjects from the outset, irrespective of the business process. The implementation of such a system is rendered unfeasible without the development of data protection awareness, a necessity which must be met by both employees and managers. It is therefore evident that, in accordance with the principles of data protection by design, the establishment of a suitable data protection governance framework serves to operationalize the requirement of data protection accountability. A framework facilitates the justification of the introduction and application of data protection controls, the documentation of risk mitigation measures, and their internal or external verification.

The chapter on the data protection officer elucidates that many companies that process data are required to have a data protection officer, or at the very least, a specialist who is knowledgeable in data protection issues and is familiar with law and data protection practice. To comply with the principle of transparency, it may be necessary to employ a professional perspective, knowledge and opinion in many cases. The guidelines issued by the working group are largely general in nature, which can result in numerous interpretation issues.

Nevertheless, the engagement of a data protection specialist within the corporate structure, particularly in SMEs, can result in a substantial financial impact, a capacity which is not universally accessible to all organizations.

The chapter on data and cyber security and incident management concludes with the unambiguous assertion that, in the today's highly interconnected digital environment, the protection of personal data has never been of such paramount importance. In the contemporary context, characterized by escalating cyber threats, the prevalence of phishing, and mounting privacy concerns, organizations are under considerable pressure to safeguard sensitive information, particularly personal data. Incident response planning, as defined by the GDPR, constitutes a pivotal element of a company's compliance strategy, playing a crucial role in minimizing the damage resulting from a data breach

and ensuring rapid recovery. It is also imperative to devise an incident management policy that delineates the procedures for the identification, reporting, escalation, and resolution of incidents. In the context of SMEs, the predominant challenge in incident management pertains to the identification of incidents, which is predominantly attributable to a paucity of data protection awareness. As previously stated, employee awareness is paramount in this regard, given that employees frequently constitute the primary line of defense in the prevention or identification of potential incidents. The second most common problem is the failure to report and record incidents. This is due to organizations considering economic interests and therefore fearing potential fines or reputational damage that may result from reporting an incident. However, it is essential to emphasize that, without the development and adherence to appropriate incident management procedures, the concept of full data protection compliance remains unattainable.

A further salient issue pertains to the frequent failure of decision-makers to acknowledge the significance of IT data security. Moreover, the scarcity of resources allocated to the development of security systems further exacerbates the situation.[8]

The chapter on data subject rights demonstrates that individuals are granted greater insight and rights regarding to the processing of their data, while companies have increased obligations in this regard. It is evident that adhering to the rights of data subjects and providing a timely response to their requests, as stipulated in the GDPR, results in a substantial increase in the cost of compliance. Conversely, in instances of unlawful data processing, data subjects retain the right to initiate civil lawsuits, invoking the provisions of the Civil Code. Furthermore, in the context of the right to the protection of personal data, which is enshrined in the personality rights enumerated under the Civil Code, data subjects are also entitled to claim damages. Consequently, SMEs are also subject to civil liability regarding data protection breaches.

Regarding the issue of contractual liability, it is evident that organizations are not only accountable for the security of the personal data they process but also obligated to ensure that any external organization with which they share personal data implements rigorous security measures to guarantee an adequate level of protection of personal data. Consequently, a significant obligation incumbent upon the data controller is to select contractual partners (data processors or joint data controllers) who are not only proficient from a professional standpoint but also provide adequate guarantees with regard to data protection, and to precisely delineate the responsibilities pertaining

[8] Dr. Zemplenyi Adrienne, *op. cit.,* 5.p.

to data processing. The utilisation of meticulously formulated data processing agreements has been demonstrated to facilitate not only the assurance of compliance but also the establishment of a culture of trust between business partners, thus promoting accountability.

Moreover, in order to ensure the lawfulness of data processing, it is necessary for all data processing operations to have a legal basis in accordance with the law. This poses a significant challenge, particularly for small and medium-sized enterprises. As previously stated, these challenges primarily stem from limited resources, a paucity of expertise, and the complexity of compliance requirements.

Despite the fact that the GDPR delineates six legal bases for data processing, SMEs frequently encounter difficulties in identifying and employing the appropriate legal basis with precision. This predicament often arises from their lack of dedicated legal or data protection professionals, resulting in errors or omissions in the selection and justification of the legal basis. Consequently, there is frequently an over-reliance on consent as the ostensibly simplest solution.

However, the distinction between contractual consent and consent under the GDPR as a legal basis for processing personal data is critical to understanding the complexity of data protection and contractual obligations in today's digital economy.

In accordance with Section 6:58 of the Hungarian Civil Code, a contract is defined as a mutual and consistent legal statement by the parties involved, which establishing an obligation to provide a service and a right to receive a service in return.

In this particular instance, the declaration of will (contractual consent) intended to engender legal effects encompasses on the one hand, the intention of the civil law subject and the means of expressing it, in the form of a statement made orally, in writing, or by conduct that indicates it.[9]

Accordingly, contractual consent can be defined as an agreement between the parties, based on which the parties undertake to accept the provisions included in the contract.

In contrast, consent under the GDPR, which is defined as "freely given, specific, informed and unambiguous" (GDPR, 2016), serves primarily to protect the rights of the data subjects and ensure their autonomy in deciding on the processing of their personal data.

---

[9] Juhász Ágnes: A szerződéses akarat és annak egyes értelmezési kérdései, különös tekintettel a szerződés részleges érvénytelenségére, Miskolci Jogi Szemle, 17. évfolyam (2022) 2. szám (1. különszám), https://doi.org/10.32980/MJSz.2022.2.2008, 190.p.

The data processing conditions included in the contract may give the impression that the data subject, by signing the contract, gives his consent to the processing of data pursuant to Article 6(1)(a). Conversely, the data controller may erroneously infer that the execution of the contract signifies consent, as interpreted under Article 6(1)(a). It is imperative to acknowledge, however, that these are two discrete concepts. It is imperative to draw a distinction between the acceptance of the terms of service that serves to conclude a contract, and the consent to specific data processing as outlined under Article 6(1)(a). These two concepts entail different requirements and legal consequences. It is also worth note that the modification of data processing purposes can result in a concomitant alteration to the legal basis. This may prove to be a challenge for companies, who may find it difficult or impossible to recognize such changes.

As demonstrated by the case law,[10] he articles most frequently violated are Articles 5, 6, and 32. This suggests that companies encounter difficulties complying with the general principles of data processing, obtaining valid consent, selecting the appropriate legal basis, and implementing security measures. These challenges are attributable to the complexity of the GDPR requirements, which engender a substantial administrative burden.

Finally, it is evident that artificial intelligence has engendered a paradigm shift in the operations and customer interactions of businesses of all sizes. While substantial corporations have the capacity to expeditiously implement artificial intelligence (AI) technologies, the financial burden of investing in associated cybersecurity measures, encryption technologies, and ensuring compliance with data protection regulations can prove prohibitive for SMEs.

In the course of the research, four principal challenges for SMEs in terms of compliance processes were identified: namely, technical, legal, organizational, and legal interpretation challenges. Within each category, a range of issues can be identified, including resource constraints, the challenge of modifying corporate culture, difficulties in collaborating with partners and the complexity of interpreting and understanding the regulation. The challenges identified in the study demonstrate the multifaceted nature of GDPR compliance, particularly in view of the vast amount of personal data collected, processed, and stored in today's technologically advanced and interconnected world. Considering the considerations, it is evident that the average SME lacks the

[10] Statista, Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/.

requisite human and financial resources to allocate to data protection compliance. Consequently, these entities generally do not aspire to attain a high level of data protection compliance.

List of publications on the subject of the thesis

Boros Anita: Obținerea consimțământului persoanei vizate în teorie și în practică, Jurnalul Baroului Cluj, 01/2022 44-60. p., https://www.baroul-cluj.ro/wp-content/uploads/2022/07/boros.pdf.

Boros Anita: Adatvédelmi megfelelés: privacy by design és a hatásvizsgálat mint az elszámoltathatóság eszközei, Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2020. 7-28. o.

Boros Anita: Az adatvédelmi tisztviselő mint az elszámoltathatóság sarokköve, Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2022, DOI: 10.55052/themis.2022.2.6.32.

Boros Anita: Principiul responsabilității în prelucrarea datelor cu caracter personal, Jurnalul Baroului Cluj, 02/2021, https://www.baroul-cluj.ro/wp-content/uploads/2021/12/boros.pdf.

Boros Anita: Jogos érdek mint az adatkezelés jogalapja az elméletben és a gyakorlatban Themis: Az Elte Állam- és Jogtudományi Doktori Iskola elektronikus folyóirata, 2021, 7-33. p.

Boros Anita: Issue of cookie consent in the light of applicable eu laws, RODOSZ konferenciakötet, Kárpát-medencei Magyar Doktoranduszok Interdiszciplináris konferenciája, Társadalom és Innováció, 2020.

Boros Anita: A web-sütik használatának adatvédelmi kérdései, Pro Futuro - A jövő nemzedékek joga, Évf. 10 szám 3 (2020), https://doi.org/10.26521/PROFUTURO/2020/3/8746.

The theses are based on the following literature:

Dr. Zemplenyi Adrienne, A KKV-k tapasztalatai a GDPR alkalmazásával kapcsolatban, STARII záró konferencia, https://naih.hu/files/dr-Zemplenyi-Adrienne_A-KKV-k-tapasztalatai-a-GDPR-alkalmazasaval-kapcsolatban_STARII-zarokonferencia.pdf

European Commision, Annual Report on European SMEs 2023/2024, Luxembourg: Publications Office of the European Union, 2024.

Jon Suarez -Davis, Data isn't 'the new oil' - it's way more valuable than that, https://www.thedrum.com/opinion/2022/12/12/data-isn-t-the-new-oil-it-s-way-more-valuable

Juhász Ágnes: A szerződéses akarat és annak egyes értelmezési kérdései, különös tekintettel a szerződés részleges érvénytelenségére, Miskolci Jogi Szemle, 17. évfolyam (2022) 2. szám (1. különszám), https://doi.org/10.32980/MJSz.2022.2.2008

Nisha Talagala, Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,entity%20that%20drives%20profitable%20activity.

Polyák Gábor, Szőke Gergely László: Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2704/1967.

Statista, Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/

T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, Data Protection: CJEU case law review – 1995-2020, https://www.dpcuria.eu/case-law-review-1995-2020.pdf.https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/

Statista, Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range, https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/,

T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt, Data Protection: CJEU case law review – 1995-2020, https://www.dpcuria.eu/case-law-review-1995-2020.pdf.