EÖTVÖS LORÁND UNIVERSITY FACULTY OF LAW
DOCTORAL SCHOOLE

Boros Anita

THE LEGAL AND BUSINESS CHALLENGES OF DATA PROTECTION COMPLIANCE

PHD DISSERTATION
THESES

Supervisor: Balogh Zsolt György

Budapest,
2025

1. Summary of the research task

Data protection law is one of the most dynamically evolving areas of law, constantly challenging legislators. In the 21st century, digital transformation is inevitable, more and more business and personal lives move into digital world. Most startups have no physical space, and in this arena, data is knowledge, and knowledge is power. As the British mathematician Clive Humby said in 2006, "data is the new oil,"[1] with information being one of the most important resources. In fact, it's no exaggeration to say that having large amounts of data is now more valuable than oil. Therefore, ensuring an adequate level of data protection is very important in this modern economy.[2]

Accordingly, data asset management is an important element of corporate strategies and innovations. Companies that purposefully use the opportunities offered by big data and are better able to utilize, store and manage data, as well as share it with those responsible and protect it from unauthorized parties can gain a significant competitive advantage.

At the same time, the volume and impact of causes related to private life are increasing. The European Union legal system has already imposed strict rules on the processing of personal data and defines sanctions against those who do not act lawfully during data processing. More and more cases have come before the European Court of Justice that conflict with the right to privacy and business interests.[3] This also shows that the security of our data is becoming increasingly important. In many cases, however, technological development dictates a pace that legislation cannot keep up with, [4] so it can happen that while the corporate sector quickly takes advantage of the excellent opportunities it offers, individuals are left without tools to protect their privacy. The precise creation of data protection provisions and the definition of sanctions was initially in the hands of the member states, considering the provisions of the European Union Data Protection

---

[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.

Directive. Thus, the digital market situation began to be distorted in Europe, since the regulation was not completely uniform 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 about 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 relevance of my research topic is therefore justified by the General Data Protection Regulation (GDPR), which aims to create a single digital market and modernize the regulation of security and citizen self-determination issues related to the processing of personal data.

My research responds 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. However, considering that SMEs account for 99% of businesses[5] in the European Union, the success of data protection regulation is largely reflected in the level of compliance of SMEs.

With the introduction of the new General Data Protection Regulation, uncertainties surrounding data protection rules do not cease to exist, and enforcing compliance with the unified regulation is a complicated task due to the numerous general formulations of the regulation.

Due to the specific situation of different geographical regions or even industries, the level of compliance with the rules of the regulation, or the extent of compliance with the rules, may differ. This study sets itself no less a goal than to demonstrate that for companies with limited resources and information management systems, data protection compliance means a lot of work and a serious financial burden, since in addition to complying with the existing data management rules, it introduces new obligations for data controllers and processors that require the development of time-consuming and costly processes. One example is the principle of accountability, which transfers responsibility from national authorities to organizations and obliges them to demonstrate full compliance with the legislation. This is a serious responsibility, especially for companies that

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

handle large amounts of personal data, as compliance is not only a legal issue, but also comprehensively affects process management, control environment and business processes, and also poses challenges in many areas, such as data management related to employees, which already takes into account working from home, using one's own device, online marketing, not to mention international trade and cooperation, which requires the transfer of personal data outside the European Union.

Considering the current data protection regulations, the hypothesis of this research can be formulated as follows: for a small or medium-sized company, it is not possible to devote sufficient time and resources to achieving a high level of data protection compliance.

2. Methodological approach to the dissertation

To support my hypothesis, in this study I present 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, I discuss the positions, guidelines, 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. I also analyze the fines imposed by several national authorities, which help to understand the positions of data protection authorities and to reveal the areas where data protection compliance is least successful.

My further goal is to explore the interpretation issues and shortcomings of the new data protection regulation. By comparing the legal issues that arise, I will create a comprehensive picture of the consequences of the European uniform regulation, and then I will also discuss what future problems we may encounter in the field of data protection and what possible solutions exist.

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

At the same time, I intend to rely heavily on source analysis and secondary data analysis in the study, primarily on legal sources, international treaties, laws, regulations, the jurisprudence of judicial and other law enforcement bodies, and the relevant legal literature. The aim of the research is to explore the drivers of our data protection rules and to understand the regularities. I will not emphasize generality, but rather specifics, so using the deductive method, I will determine

increasingly specific findings from general findings. This will be followed by a summary of the characteristics of the cases drawn from literature and the formulation of theoretical conclusions.

The first chapter of the thesis explores the relationship between the right to privacy and data protection and then aims to provide a comprehensive picture of the effects of data protection regulation, listing its positive and negative consequences. After that, the thesis is divided into two large parts. In the first part, we analyze the obligations specified in the Data Protection Regulation, during which we address potential compliance difficulties and interpretation issues in relation to each obligation. In the second part of the thesis, we focus on the practical challenges most frequently encountered during compliance.

Considering the rapid spread and development of artificial intelligence, I considered it essential to also analyze data protection issues related to artificial intelligence in the thesis.

3. Outcome of the research and its possible applications

Conducting the research provides the opportunity to draw lessons that can provide real assistance to companies in data protection compliance. Throughout the thesis, we strive to explore not only the interpretation issues of the regulation, but also to find answers to them.

Secondly, in addition to discussing the legal requirements, I also formulate useful practical advice, which can be a basis for companies to develop their appropriate processes and information systems. In the practical challenges chapter, areas that affect most companies are analyzed, since overcoming the online presence and the data protection challenges associated with data management, as well as complying with data management in the workplace, is the first step on the path to data protection compliance.

My thesis points out that conducting successful data protection compliance is a complex task. The data controller must constantly keep up with changes in interpretation and law, monitor potential threats from both external and internal factors, ensure compliance with existing or compliance-related organizational practices, respond to stakeholder questions, and above all, have leadership skills that ensure the appropriate attitude within the organization.

From the perspective of SMEs, the introduction of data protection rules is often just another task, obligation imposed on businesses, as well as a cost and expense that may even put them at 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* also show that, as part of data protection compliance, the principles of data protection regulation must be incorporated into data processing technologies, both during design and operation. Technology must be designed and implemented in such a way that its entire life cycle can be implemented in a way that is compatible with the fundamental rights and values that define our democratic societies. However, carrying out an impact assessment, like introducing data protection by design into the corporate culture, cannot be considered a standard obligation that can be fulfilled in the same way for all companies. Data controllers must decide on the application of appropriate organizational and technical measures on a case-by-case basis, which may depend on the size of the organization, its target group or even its core activity. Data protection by design is a strategy, the cornerstone of a long-term plan, which requires respect for data protection principles and the rights and freedoms of data subjects from the very first step, regardless of the business process. All this is impossible without developing data protection awareness, which both employees and managers need to acquire. Therefore, with due regard to the principles of data protection by design,

---

[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.

the introduction of an appropriate data protection governance framework operationalizes the requirement of data protection accountability. A framework makes it possible to justify 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 makes it clear that most companies that process data need a data protection officer, or at least a specialist who is knowledgeable in data protection issues and is familiar with the law and data protection practice. To comply with the principle of transparency, a professional perspective, knowledge, and opinion may be needed in many cases. The guidelines issued, but also those of the working group, are mostly of a general nature, which can lead to many interpretation issues.

Despite all this, calling in a data protection specialist into the corporate structure, especially in SMEs, means a serious financial impact, which is clearly not something that every organization can afford.

The clear conclusion of the chapter on *data and cyber security and incident management* is that in today's highly interconnected digital environment, the protection of personal data has never been so critical. With increasing cyber threats, phishing and privacy concerns, organizations are under immense pressure to protect sensitive information, especially personal data. Incident response planning, as defined by the GDPR, is a key element of a company's compliance strategy, playing a crucial role in minimizing the damage resulting from data breach and ensuring rapid recovery. It is also critical to create an incident management policy that details how incidents are to be detected, reported, escalated and resolved. When it comes to incident management, the primary challenge in the SME sector is incident identification, which is mostly due to a lack of data protection awareness. Employee awareness, as already mentioned, plays a key role here, as employees are often the first line of defense in preventing or identifying potential incidents. The second most common problem is the failure to report and record incidents, as organizations, considering economic interests, fear potential fines or reputational damage that may result from reporting an incident. However, without developing and adhering to appropriate incident management procedures, we cannot speak of full data protection compliance.

Another key problem is that decision-makers often do not recognize the importance of IT data security, and the resources to develop such security systems are often lacking.[8]

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

The chapter on *data subject rights* shows that individuals are given greater insight and rights in relation to the processing of their data, while companies have increased obligations in this regard. Respecting the rights of data subjects and responding to their requests appropriately and within the time limits set out in the GDPR also significantly increases the cost of compliance.

At the same time, in the event of unlawful data processing, data subjects can enforce claims for damages in civil law proceedings, citing the provisions of the Civil Code. In addition, in the case of the right to the protection of personal data, which is enshrined in the personality rights listed under the Civil Code, data subjects can also claim damages. Therefore, SMEs are also subject to civil liability in relation to data protection breaches.

In relation to *contractual liability,* we can observe that organizations are not only responsible for the security of the personal data they process but also must ensure that any external organization with which they share personal data implements strict security measures to ensure an adequate level of protection of personal data. Based on this, one of the important obligations of the data controller is to select contractual partners (data processors or joint data controllers) who are not only outstanding from a professional point of view but also provide adequate guarantees in terms of data protection, and to precisely define the responsibilities related to data processing. Well-drafted data processing agreements can not only help ensure compliance but are also an essential document for accountability and can help to establish a culture of trust between business partners. Furthermore, to ensure the lawfulness of data processing, all data processing operations must have a legal basis in accordance with the law, which poses many challenges, especially for small and medium-sized enterprises. As I emphasize, these challenges mainly arise from limited resources, lack of expertise and the complexity of compliance requirements.

Although the GDPR provides six *legal bases for data processing*, SMEs often struggle to identify and correctly use the appropriate legal basis, as they often do not have dedicated legal or data protection professionals, which leads to errors or omissions in the selection and justification of the legal basis. As a result, they are often observed to over-rely on consent as the seemingly 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.

According to Section 6:58 of the Hungarian Civil Code, a contract is a mutual and consistent legal statement of the parties, which gives rise to an obligation to perform a service and a right to demand a service.

In this case, the declaration of will (contractual consent) intended to produce legal effects includes, 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 refers to 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 must be *"freely given, specific, informed and unambiguous"*, serves primarily to protect the rights of the data subjects and ensure their autonomy in deciding on the processing of their personal data.

The data processing conditions included in the content of 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). At the same time, the data controller may mistakenly assume that signing the contract corresponds to consent within the meaning of Article 6(1)(a). It is important to note, however, that these are two completely different concepts. A distinction should be made between the acceptance of the terms of service to conclude a contract and the consent to specific data processing under Article 6(1)(a), as these concepts entail different requirements and legal consequences. It can also be challenging that changed data processing purposes also entail a change in the legal basis, which companies may find difficult or impossible to recognize.

As the case law shows,[10] the most violated articles are Articles 5, 6 and 32, indicating that companies struggle with complying with the general principles of data processing, obtaining valid consent, choosing the right legal basis and implementing security measures. These challenges arise from the complexity of the GDPR requirements, which leads to a significant administrative burden.

Finally, we can also observe that *artificial intelligence* has brought change to businesses of all sizes, revolutionizing the way companies operate and interact with customers. While large companies can quickly implement AI technologies, investing in related cybersecurity measures,

---

[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.

[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/.

encryption technologies and ensuring compliance with data protection rules can be prohibitively expensive for SMEs.

During the research, we identified four main challenges for SMEs in terms of compliance processes: technical, legal, organizational and legal interpretation challenges. Within each category, we can observe different problems, such as resource constraints, the difficulty of changing corporate culture, difficulties in collaborating with partners and the complexity of interpreting and understanding the regulation. The challenges identified in the study clearly demonstrate the multifaceted nature of GDPR compliance, considering the vast amount of personal data collected, processed and stored in today's technologically advanced and interconnected world. Taking all this into account, it becomes clear that the average SME does not have adequate human and financial resources to devote to data protection compliance and therefore does not usually strive to achieve a high level of data protection compliance.

4. 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.