A Regulatory Analysis of *Cybersecurity* Policy and *Data Protection* Policy

TABLE OF CONTENTS

I. Introduction

Digital transformation represents a paradigm shift that fundamentally reimagines business processes, customer experiences, and operational models through the integration of advanced technologies including cloud computing, artificial intelligence, machine learning, and Internet of Things (IoT) devices.[1] This shift is not merely technological but strategic, as it enables organizations to increase efficiency, improve decision-making, and remain competitive in rapidly evolving markets. Despite their benefits in driving innovation and efficiency, these technologies expand the cybersecurity landscape in ways that exceed the capabilities of traditional security frameworks, exposing organizations to evolving and more sophisticated threats. The global cybersecurity market is projected to reach $345.4 billion by 2026, reflecting the critical importance of security in digital transformation initiatives.[2] Organizations worldwide are experiencing an average of 4,000 cyberattacks daily, with the cost of data breaches reaching $4.45 million per incident in 2023.[3] Regulatory requirements are also evolving. For example, the European Union's General Data Protection Regulation (GDPR), along with similar laws in other regions, has placed greater pressure on organizations to place a stronger emphasis on protecting data privacy and ensuring security. The purpose of this paper is to analyze how cybersecurity policies support compliance with data protection laws, with particular reference to regulatory frameworks such as GDPR, and to evaluate the role of organizational practices in aligning technical security measures with legal obligations.

II. Legal and Conceptual Framework

II.1 Evolution of Cyber Terminology

[1] Westerman G, Calméjane C, Bonnet D, Ferraris P, McAfee A. Digital Transformation: A Roadmap for Billion-Dollar Organizations. Cambridge: MIT Center for Digital Business and Capgemini Consulting; 2011

[2] Fortune Business Insights. Cybersecurity Market Size, Share & COVID-19 Impact Analysis. Pune: Fortune Business Insights; 2022.

[3] IBM Security. Cost of a Data Breach Report 2023. Armonk: IBM Corporation; 2023.

The terms *cyber*, *cyberspace*, and *cybersecurity* have evolved from earlier cultural and academic contexts into mainstream usage. Early references include Norbert Wiener's concept of cybernetics, which described the control and communication of complex systems, as well as William Gibson's depiction of cyberspace as a "consensual hallucination" representing networked digital environments in *Neuromancer*.

II.2 Definition and Core Objectives of Cybersecurity

Over time, these ideas, along with various cultural influences, have contributed to the widespread and multifaceted use of cyber-related terminology today.[4] We can say that the activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation represents the core objective of cybersecurity, emphasizing the protection of systems and data through measures that ensure confidentiality, integrity, and availability.[5]

II.3 Legal Foundations of Data Protection

The right to data protection is closely linked to the broader right to privacy, as it is embedded within international human rights frameworks.

II.3.1 European Convention on Human Rights (Article 8)

For instance, under Article 8 of the European Convention on Human Rights (ECHR), individuals are protected against unjustified collection and use of personal data as part of their right to respect for private and family life, home, and correspondence. Over time, data protection has developed through various legal instruments, including early international recognition in the Universal Declaration of Human Rights, which influenced later European frameworks. Within Europe, the

[4] European Union Agency for Cybersecurity (ENISA). (2021, December). *Definition of cybersecurity: Gaps and overlaps in standardisation (v1.0)*. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf

[5] Vishik, C., Matsubara, M., & Plonk, A. (2016). Key concepts in cyber security: Towards a common policy and technology context for cyber security norms. In A.-M. Osula & H. Rõigas (Eds.), *International cyber norms: Legal, policy & industry perspectives* (pp. 221–242). NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch11.pdf

Council of Europe established Convention 108 as the first legally binding international treaty specifically focused on data protection, while the European Union later addressed the issue through its Data Protection Directive and subsequent legal developments. Today, data protection is recognized not only as a regulatory requirement but also as a fundamental right, with institutions such as the European Court of Human Rights interpreting and enforcing obligations that require states to both avoid unlawful interference and, in certain cases, take active steps to protect individuals' privacy.

II.4 Relationship Between Cybersecurity and Data Protection

A global landscape on data protection regulations designed to protect consumer rights has emerged within the last ten years with the adoption of national regulations. In 2011, there were only 76 countries that had enacted data privacy laws, and by 2019, that number had increased to 132 countries.[6] Data Protection requires two parts, a legal framework and technical standards. Regulations are often complex as it affects society, economic development, and national security. On the one hand, data protection legislation poses a challenge to lessen data flow in a world driven by data analytics. On the other hand, it poses a positive change to increase consumers' trust and increase innovations that could provide possible safeguard personal data.[7]

III. General Data Protection Regulation (GDPR) and Its Implications

III.1 Overview and Scope of GDPR

The GDPR came into force in May 2018. It was incorporated into the Data Protection Act 2018, which replaced the 1998 Act, and places greater obligations on how organisations handle personal data. The GDPR applies to 'personal data', meaning any information relating to an identifiable person who could be directly or indirectly identified, particularly by reference to an identifier.

III.2 Data Protection Principles and Security Requirements

---

[6] Graham Greenleaf, "Global data privacy laws 2019: 132 national laws & many bills." 157 Privacy Laws & Business International Report. February 8, 2019, 14.

[7] Crispin Niebel, "The impact of the general data protection regulation on innovation and the global political economy." Computer Law & Security Review 40 (2021),12

The GDPR requires personal data to be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. The GDPR applies to processing carried out by organisations operating within the European Union (EU). It also applies to organisations outside the EU that offer goods or services to individuals in the EU.[8] The GDPR has been incorporated into UK data protection law via the EU Withdrawal Act.

III.3 Enforcement and Penalties

The GDPR includes a maximum fine of up to 4% of annual global turnover or €20 million – whichever is greater – for organisations that infringe its requirements. Supervisory authorities such as the UK's ICO can also take a range of other actions, including: [9]

- issuing warnings and reprimands
- imposing a temporary or permanent ban on data processing
- ordering the rectification, restriction or erasure of data
- suspending data transfers to third countries

Other recent research noted that changes in cyber risk management could have, in part, been attributed to the introduction of the GDPR. For example, the 2020 Cyber Security Breaches Survey[10]

III.4 Impact of GDPR on Organizational Cybersecurity Practices

A significant portion of organizations in the UK reported adjustments to their cybersecurity policies and procedures following the introduction of the GDPR, with 38% of businesses and 42% of charities indicating that they had implemented such changes. In some instances, these

[8] Information Commissioner's Office (ICO). (n.d.). *Guide to the General Data Protection Regulation (GDPR) – FAQs*.
[9] Department for Digital, Culture, Media & Sport. (2020). *Impact of GDPR on cyber security outcomes*. UK Government. https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf
[10] DCMS, Ipsos Mori and University of Portsmouth (2020) Cyber Security Breaches Survey 2020. Findings from this survey are based on a random probability telephone survey of 1,348 UK businesses and 337 UK registered charities was undertaken from 9 October 2019 to 23 December 2019

adjustments were directly linked to GDPR requirements; however, existing literature provides limited evidence assessing the overall impact of the GDPR within the UK context.

The DCMS 2019 Cyber Security Breaches Survey found that while GDPR helped improve baseline cybersecurity awareness across UK organisations, it may have also led some to view cybersecurity primarily through a data protection lens. In some cases, increased staff training in cybersecurity was driven by GDPR-related initiatives, where the focus on broader cybersecurity content was relatively limited. The findings also suggest that many organisations treated GDPR and cybersecurity as closely connected, with GDPR compliance sometimes taking priority over cybersecurity as a standalone strategic concern.[11]

Cyber security can be broken down into several different elements, including[12]:

- application security – the security of applications and software downloaded onto a computer or network
- information security - safeguarding sensitive information from illegitimate access, usage, revelation, disruption, alteration, reading, inspection, damage or recording. The GDPR is an example of information security
- network security - comprehensive security policies and provisions adopted in an adaptive and proactive manner by the network administrator for thwarting and monitoring unauthorised access
- disaster recovery/business continuity planning – the procedures in place for a business to continue operating both during and after a cyber-attack

[11] Department for Digital, Culture, Media & Sport. (2020). *Impact of GDPR on cyber security outcomes*. UK Government. https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf

[12] Cross Domain Solutions. (n.d.). *Cyber security: elements*. Cross Domain Solutions.

● end user education – educating technology users so that they are aware of best practice to protect themselves from a cyber-attack There were mixed views on the extent to which the GDPR had led to improvements across all of these areas.

III.5 International Cooperation (Budapest Convention)

A notable example of international cooperation in cyber security is the Budapest Convention, officially known as the Council of Europe Convention on Cybercrime. In fact, this is the first international treaty that deals with crimes committed through internet. It was enforced in November 2001 and any state can joint it. It lists five cyber actions illegal and these should be investigated by authorized domestic agencies. These actions are unauthorized access, unauthorized interception, data interference, system interference and misuse of devices.[13]

III.6 Limitations and Long-Term Effectiveness

There is limited evidence regarding whether the reported impacts of the GDPR on cyber security practices have, or will be, sustained. It is too soon to determine if the change in cyber security measures being reported has resulted in a longer-term behaviour change or cultural shift towards more robust practices. For example, a recent article noted that 'genuine cyber-resilience comes from corporate muscle-memory, which is developed from incident response planning with legal, communications and IT security stakeholders, and which is sustained by testing and updating processes on a regular basis.[14] Thus, cyber laws are criticized by some as "paper laws".[15]

[13] Convention on Cybercrime, Council of Europe, http://conventions.coe.int/Treaty/EN/ Reports/Html/185.htm.
[14] Information Age. (n.d.). *Cyber security breaches fall*. Information Age. https://www.information-age.com/cyber-security-breaches-fall-123481460/
[15] TASAM. (n.d.). *İGK2 Kitap*. TASAM (Turkish Asian Center for Strategic Studies). https://tasam.org/Files/Icerik/File/%C4%B0GK2Kitap_(21)_(1)_pdf_f44d71f0-a0ae-4566-a530-941ed46591cb.pdf

IV. Cybersecurity Policy, Compliance, and Implementation Challenges

IV.1 Cybersecurity Policy as a Compliance Mechanism

The European Court of Auditors [16] emphasizes that evaluating the effectiveness of EU cybersecurity policy remains a complex task due to the absence of clearly defined, measurable objectives. Many of the goals outlined in earlier strategies are broadly framed and reflect high-level ambitions rather than specific, quantifiable targets, which makes it difficult to assess progress or establish a direct causal relationship between policy actions and outcomes. As a result, measuring the true impact of these policies is inherently limited.

IV.2 Alignment Between Legal Requirements and Technical Measures

In addition, the evaluation of cybersecurity initiatives is further constrained by a lack of reliable and harmonized data across Member States. There is no common monitoring system or standardized set of indicators at the EU level, which leads to inconsistencies in how cybersecurity performance is tracked and reported. Few Member States systematically collect comprehensive data on cybersecurity-related issues, and this absence of comparable statistics reduces the ability to conduct meaningful cross-country analysis or identify broader trends. Furthermore, independent EU-wide studies covering key aspects such as cybercrime, cybersecurity economics, and system resilience remain limited.

The report also notes that progress in cybersecurity policy is often assessed in qualitative terms, focusing on activities completed or milestones achieved rather than concrete outcomes or measurable improvements. Baselines for evaluating system resilience have not been clearly established, and the lack of a unified definition of cybercrime further complicates the development of consistent indicators. Oversight and auditing practices vary significantly among Member States, with many national audit institutions having limited experience in this policy area. Where audits have been conducted, they tend to focus on areas such as governance, critical infrastructure protection, and incident response, while other important aspects like awareness-raising and skills development are less frequently examined.

---

[16] European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy: Briefing paper*. https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf

IV.3 Organizational Challenges in Implementation

Legislation alone does not guarantee resilience. While the NIS Directive's objective is to achieve a high level of security across the EU, it explicitly focuses on achieving minimum, not maximum, harmonization.[17] Gaps will continue to emerge as the cyber-landscape evolves.

The EU's capacity to respond to cyberattacks at the operational and political level in the event of a large-scale, cross-border incident has been labelled "limited", partly because cybersecurity is not yet integrated into existing EU-level crisis response coordination mechanisms.[18] The NIS Directive did not address this.

[17] Article 3, NIS Directive

[18] Cooperation over early warnings and mutual assistance need further development as well: Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 10085/18, 26 June 2018

V. Conclusion

This paper has examined the relationship between cybersecurity policy and data protection law within the context of digital transformation and the growing reliance on digital systems. As organizations adopt advanced technologies such as cloud computing, artificial intelligence, and interconnected devices, the need to protect data and systems has become more critical. At the same time, the expansion of the cyber threat landscape has made it clear that traditional security approaches alone are no longer sufficient to address modern risks.

The analysis shows that cybersecurity and data protection are closely connected, both in concept and in practice. Legal frameworks such as the European Convention on Human Rights, Convention 108, and the General Data Protection Regulation (GDPR) establish obligations for protecting personal data, while cybersecurity policies provide the technical and organizational means to meet those obligations. In this sense, cybersecurity functions as a practical tool that supports compliance with legal requirements, translating regulatory principles into operational measures such as access control, data protection procedures, and incident response planning.

The introduction of the GDPR has had a noticeable impact on organizational practices, leading many businesses and institutions to revise their cybersecurity policies, increase awareness, and invest in training. However, the findings also suggest that in some cases cybersecurity efforts are driven primarily by compliance needs rather than being developed as part of a broader, long-term security strategy. This can limit the effectiveness of such measures and create a situation where cybersecurity is treated mainly as a legal requirement rather than an essential component of organizational resilience.

At the regulatory level, significant challenges remain. Evaluating the effectiveness of cybersecurity policies is difficult due to the lack of clearly defined objectives, consistent data, and standardized measurement frameworks across Member States. Differences in implementation, limited availability of comparable statistics, and gaps in oversight further complicate the ability to assess progress. In addition, the rapid pace of technological change continues to outstrip the development of legal and policy frameworks, leaving certain areas insufficiently addressed.

Overall, while progress has been made in aligning cybersecurity policy with data protection requirements, there is still a need for stronger integration between legal standards and practical implementation. Improving coordination, establishing clearer metrics, and promoting consistent evaluation practices would help strengthen both compliance and effectiveness. A more structured and holistic approach to cybersecurity governance is therefore essential to ensure that organizations are not only meeting regulatory obligations but also building sustainable and resilient security practices in an increasingly complex digital environment.