International Journal of Innovative Solutions in Engineering
2026, Special Issue No. 1 (pages 126–138)
DOI: 10.47960/3029-3200.2026.S1.126

Preliminary Communication

OPEN ACCESS

Compliance of Technical and Organizational Data Protection Measures with the New Law on Personal Data Protection of Bosnia and Herzegovina (2025) and the NIS2 Directive: A Comparative Doctrinal and Gap Analysis

Admir Sivro[1], Jasmin Azemović[1]

[1]Faculty of Information Technologies, University Džemal Bijedić Mostar, Bosnia and Herzegovina

Abstract

Modern information systems face growing cybersecurity regulatory requirements as the EU enforces both the General Data Protection Regulation (GDPR) and the NIS2 Directive (EU 2022/2555). Although not an EU member state, Bosnia and Herzegovina adopted a new, GDPR-aligned Law on Personal Data Protection in early 2025, while regional initiatives increasingly reference NIS2 standards. This paper maps and compares the technical and organizational measures prescribed by the Bosnian law against the ten security-measure categories of Article 21 of NIS2, identifying the degree of coverage and regulatory gaps. The study used qualitative comparative document analysis, with two independent coders reviewing the primary legal texts. Results show the law conceptually addresses nine of ten categories, with a dominant pattern of partial coverage (70%): it establishes security principles but rarely reaches the technical detail required by NIS2. Only cryptography/encryption and effectiveness assessment (20%) are fully covered, while multi-factor authentication (10%) remains unaddressed. An internal asymmetry emerges within the law: more precise technical elaboration of access controls for competent authorities in the criminal-law context than for economic operators, the primary NIS2 addressees. The findings offer a basis for recommendations to BiH regulators and organizations and a starting point for future regional research.

Article history
Received: 25.8.2026.
Revised: 8.10.2026.
Accepted: 12.10.2026.

Keywords
Personal Data Protection,
NIS2,
Cybersecurity,
GDPR,
Regulatory Compliance,
Bosnia and Herzegovina.

1 Introduction

Modern information systems, regardless of the sector in which they operate, face an increasing number of cyber threats, while regulatory requirements for data protection and the continuity of critical services are also rising. Over the past decade, the European Union has established two key, yet conceptually different, regulatory frameworks that directly shape how organizations manage information system security: the General Data Protection Regulation (GDPR), primarily focused on protecting the personal data of natural persons, and Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, known as the NIS2 Directive, which has a broader, systemic orientation toward the resilience of critical infrastructure and information systems as a whole.

Bosnia and Herzegovina, although not a member state of the European Union, remains under constant pressure to align its domestic legislation with the EU acquis as part of the European integration process. In this context, the Parliamentary Assembly of Bosnia and Herzegovina adopted, in early 2025, a new Law on Personal Data Protection, published in the Official Gazette of BiH No. 12/2025 and modeled on the GDPR, whose full application began on 4 October 2025. In parallel, regional initiatives such as the one aimed at strengthening the cybersecurity resilience of the energy sector in Bosnia and Herzegovina and

Contact Admir Sivro, admir.sivro@edu.fit.ba, Faculty of Information Technologies, University Džemal Bijedić Mostar
©2026 by the Author(s). Licensee IJISE by Faculty of Mechanical Engineering, Computing and Electrical Engineering, University of Mostar. This article is an open-access and distributed under the terms and conditions of the CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/)

neighboring countries, launched in August 2025, explicitly rely on the requirements of the NIS2 Directive as a reference framework, even though BiH, as a non-EU member, has no formal obligation to transpose it.

This situation creates a specific and still insufficiently researched problem: organizations in Bosnia and Herzegovina de facto face two parallel sets of expectations regarding technical and organizational security measures, one arising from the domestic Law on Personal Data Protection, and another which, through regional initiatives and the future prospects of European integration, increasingly relies on NIS2 standards. At the same time, there is no systematic, publicly available analysis showing the extent to which these two frameworks overlap, and where substantive gaps exist that domestic organizations and regulators should address.

This problem is not purely theoretical. Official EU-level guidance confirms substantial structural overlap between the two frameworks: the European Union Agency for Cybersecurity (ENISA) has published technical implementation guidance for the NIS2 Directive's Article 21 risk-management measures that closely mirrors security controls organizations already apply to comply with Article 32 of the GDPR (encryption, access control, incident-handling procedures, and business-continuity planning) [1], and a detailed article-by-article mapping of the interplay between the two instruments shows that they intersect across incident-reporting obligations, breach-notification duties, and the security of processing operations, while also foreseeing coordination between NIS2 competent authorities and GDPR supervisory authorities to avoid duplicate sanctioning for the same conduct [2]. The remaining difference primarily relates to NIS2's more explicit requirements concerning supply chain security, vulnerability disclosure policies, and crisis management protocols. If this pattern of overlap and divergence is applied to the context of the new Bosnian law, the question arises as to how far that law alone is sufficient as a basis for future compliance with the broader cybersecurity requirements for critical infrastructure or whether it leaves gaps that organizations and regulators in BiH do not currently recognize.

The aim of this paper is to systematically map and compare the technical and organizational measures prescribed by the new Law on Personal Data Protection of Bosnia and Herzegovina with the ten categories of security measures prescribed by Article 21 of the NIS2 Directive, and, on the basis of this analysis, to identify the degree of coverage and the concrete gaps relevant to organizations and policymakers in Bosnia and Herzegovina.

Accordingly, this paper asks: To what extent do the technical and organizational measures prescribed by the new Law on Personal Data Protection of Bosnia and Herzegovina (2025) cover the requirements of the NIS2 Directive, and which categories of security measures represent the largest regulatory gap in the domestic context?

The paper is structured as follows: Section 2 provides an overview of the relevant literature and regulatory framework; Section 3 describes the methodology of the comparative analysis; Section 4 presents the results of the mapping exercise; Section 5 discusses the findings and their implications; Section 6 presents the conclusions, research limitations, and directions for future work.

2 Literature Review

2.1 GDPR and Technical/Organizational Data Protection Measures

The General Data Protection Regulation (GDPR) [3], in force since 2018, established the reference framework for protecting the personal data of natural persons within the European Union, directly influencing non-EU countries seeking to align with European standards. Article 32 of the GDPR requires data controllers and processors to implement “appropriate technical and organizational measures” taking into account the nature, scope, context, and purpose of processing, as well as the risks to the rights and freedoms of natural persons. This deliberately technology-neutral formulation leaves room for interpretation while also establishing principles that, in practice, translate into concrete

controls: encryption, access control, regular security testing, and the ability to restore data availability promptly after an incident. This translation of a high-level, technology-neutral principle into concrete, verifiable technical requirements has also been examined from a requirements-engineering perspective, which decomposes the GDPR's obligations into more specific architectural and organizational constraints and highlights the interpretative work this translation requires in practice [4], a challenge that, as shown later in this paper, is equally present in the new BiH Law.

2.2 The NIS2 Directive and Its Security Framework

The NIS2 Directive [5], which entered into force on 16 January 2023 as the successor to the original NIS Directive of 2016, significantly expands the sectoral scope and security requirements for entities classified by the EU as “essential” or “important.” Article 21 of the Directive prescribes ten categories of mandatory risk-management measures, including risk-analysis policies, incident handling, business continuity, supply chain security, security in system acquisition and development, assessment of the effectiveness of measures, cyber hygiene and training, cryptography, human resources security and access control, and the use of multi-factor authentication. These requirements are further technically elaborated by Commission Implementing Regulation (EU) 2024/2690 [6], which specifies concrete technical sub-requirements for digital infrastructure and ICT service providers. It should be noted that the Implementing Regulation's direct binding scope within the EU is limited to these specific digital-infrastructure and ICT-service-provider subsectors, rather than to all NIS2-covered entities; it is nonetheless treated in this paper as an authoritative technical benchmark for Article 21 across sectors, consistent with its function of elaborating the general risk-management measures that Article 21 itself imposes horizontally. Beyond its technical requirements, the Directive has also been analyzed through the lens of "digital sovereignty," with recent research arguing that NIS2 should be understood not merely as a cybersecurity instrument but as part of the EU's broader strategy to reduce dependency on non-European digital infrastructure and technology providers [7], a framing that is also indirectly relevant to non-EU states such as BiH, whose critical infrastructure often depends on the same regional and international technology supply chains.

A systematic literature review on the NIS2 Directive conducted by Ruohonen [8] shows that existing research predominantly addresses the Directive in combination with other EU cybersecurity laws, and that the majority of studies focus on industrial control systems, telecommunications, and the energy and water sectors. The author explicitly notes that, despite the extensive existing literature, significant research gaps remain, particularly regarding the practical implementation of the Directive outside the borders of the EU. Similarly, Shamatonova [9] analyzes the challenges the NIS2 Directive poses for organizations, emphasizing the burden the new regulation represents for smaller organizations with limited resources, a finding particularly relevant to countries such as Bosnia and Herzegovina.

2.3 Overlap between the GDPR and the NIS2 Directive

The question of overlap and complementarity between the GDPR and the NIS2 Directive is receiving increasing attention in the literature and in regulatory practice, since both regulations require documented security measures, incident reporting, and management-level accountability. The European Union Agency for Cybersecurity (ENISA) has published technical implementation guidance for the measures required under Article 21 of the NIS2 Directive that closely parallels the security controls organizations already apply to comply with Article 32 of the GDPR [1], and an authoritative article-by-article mapping of the interplay between the two instruments confirms substantial overlap in incident-reporting obligations, breach-notification duties, and processing-security requirements [2]. The remaining difference primarily concerns explicit NIS2 requirements relating to supply chain security, vulnerability disclosure policies, and crisis-management protocols, elements that go beyond the narrower, data-centric scope of the GDPR. This pattern is not unique to the GDPR-NIS2 pair: a recent mapping analysis of the EU's Cyber Resilience Act

against the GDPR similarly found substantial overlap in confidentiality, integrity, and availability guarantees, data minimization, traceability, and security-testing obligations across recently adopted EU digital-regulation instruments, while also identifying genuinely new, non-overlapping requirements [10]. More broadly, a systematic mapping study of GDPR-derived data-protection requirements confirms that such regulatory overlap and requirement repetition is a recurring, structural feature of EU cybersecurity and privacy legislation rather than an isolated coincidence [11]. This finding forms the starting point for the proposed research methodology, since the same logic of overlap and divergence can be applied to comparing the NIS2 Directive with the new Bosnian Law on Personal Data Protection.

2.4 Cybersecurity and Regulatory Compliance in the Western Balkans

The regional context of the Western Balkans is characterized by gradual, yet uneven, alignment with European cybersecurity standards. A regional initiative launched in August 2025, aimed at strengthening the resilience of the energy sector in Albania, Bosnia and Herzegovina, Montenegro, and North Macedonia, explicitly relies on the NIS2 Directive as a reference framework, despite the fact that none of these countries has a formal obligation to transpose it [12]. Similarly, a report from the April 2026 Western Balkans regional cyber-policy dialogue notes that countries in the region have adopted new laws aligned with the NIS2 Directive, introducing clear obligations for incident reporting, risk management, and regular audits of critical information infrastructure [13]. For comparison, official EU-level monitoring shows that, even among EU member states themselves, national transposition of the NIS2 Directive has been slow and highly uneven, with a considerable share of countries still lacking full transposition years after the formal deadline [14], [15]; this suggests that the coverage gaps identified later in this paper for BiH are part of a broader European pattern of uneven cybersecurity-law implementation rather than a uniquely domestic shortcoming.

At the academic level, Kepuska and Tomasevic [16] directly address security challenges in the Western Balkans context, showing that higher-education institutions in the region are characterized by a pronounced lack of incident-response plans and proposing a "lightweight" framework of proactive controls adapted to the region's resource constraints. Although their research focuses on the higher-education sector, the finding that formalized security frameworks are lacking and resources are limited is also relevant to the broader regional context of aligning with NIS2 requirements.

Comparative evidence from outside the Western Balkans further illustrates that formal regulatory alignment with an EU-inspired framework does not automatically translate into immediate operational clarity. An empirical study from Croatia, an EU member state that has applied the GDPR since 2018, found that the number of data protection requests submitted by academic and research institutions to the national supervisory authority increased substantially only after enforcement began, indicating a delayed and uneven adjustment process even within the Union [17]. Outside the EU altogether, a recently proposed "coverage gap" methodology has been used to benchmark a non-EU country's cyber-disclosure framework against the requirements of the USA, the EU, and the UK, revealing that formally adopted obligations were, in practice, only marginally implemented by regulated entities [18]. Both cases support the expectation, further developed in Sections 3–5 below, that a textual, doctrinal mapping of the new BiH Law is a necessary first step that should subsequently be complemented by empirical, implementation-level research.

2.5 The New Law on Personal Data Protection of Bosnia and Herzegovina (2025)

The Law on Personal Data Protection of Bosnia and Herzegovina, adopted in early 2025 and published in the Official Gazette of BiH No. 12/2025 [19], represents the most significant reform of this field in BiH to date, modeled on the GDPR and the EU Police Directive [20]. In Articles 26 and 27, the Law requires data controllers to implement appropriate technical and organizational measures with regard to the nature, scope, and risks of processing, including the

concept of data protection by design and by default [20]. Furthermore, the Law introduces an obligation to report personal data breaches to the BiH Personal Data Protection Agency within 72 hours of becoming aware of an incident, as well as an obligation to maintain records of processing activities [21]. The Law's full application began on 4 October 2025, following a 210-day transitional period [21].

2.6 Identified Research Gap

The literature review reveals a clear gap: while there is a growing body of academic and institutional literature on the overlap between the GDPR and the NIS2 Directive within the EU context [1], and while fragmentary literature exists on cybersecurity in the Western Balkans context [16], [12], [13], there is no systematic academic analysis that explicitly maps the provisions of the new Bosnian Law on Personal Data Protection against the requirements of the NIS2 Directive. This gap is particularly significant given that the Law entered into full application only a few months before this paper was written, opening a window for timely scholarly analysis that could inform future regulatory and organizational decisions in Bosnia and Herzegovina. This paper seeks to address this gap precisely.

3 Methodology

3.1 Research Approach

The research uses qualitative comparative document analysis, a methodological approach common in legal-technical research on regulatory compliance, in which the content of two or more normative texts is systematically compared according to predefined categories. This approach was chosen instead of an empirical (e.g., survey- or experiment-based) study for two reasons: (1) the object of analysis is the legal and regulatory texts themselves, whose precise interpretation is a prerequisite for any subsequent empirical assessment of implementation in practice, and (2) the limited time available for the preparation of this paper, given that the Law entered into force only a few months before the research was conducted, which precludes the collection of reliable empirical data on its actual application within organizations. This research is therefore conceived as the first, foundational phase of a broader research program.

3.2 Data Sources

The analysis is based on the following primary sources:

- The Law on Personal Data Protection of Bosnia and Herzegovina (Official Gazette of BiH, No. 12/2025) [19], the full text of the law, with particular focus on the provisions relating to technical and organizational security measures for data processing (Arts. 26–27), incident reporting, records of processing activities, and controller/processor responsibilities.
- The NIS2 Directive (Directive (EU) 2022/2555) [5], with a focus on Article 21 (cybersecurity risk-management measures), which defines ten categories of mandatory measures.
- Commission Implementing Regulation (EU) 2024/2690 [6], which technically elaborates the requirements of Article 21 of the NIS2 Directive for digital infrastructure and ICT services. Although the Implementing Regulation is directly binding only for these subsectors, it was used in this analysis as an authoritative technical benchmark for interpreting the operational content of Article 21 generally, given the absence of an equivalent, more broadly binding technical elaboration.

Secondary sources (the ENISA analysis of the GDPR/NIS2 overlap [1], academic literature [8]–[22]) were used to validate the categorization and to contextualize the findings, but not as a basis for the mapping itself, which relies exclusively on the primary legal texts.

3.3 Mapping Framework

The structure of the ten categories of measures set out in Article 21(2) of the NIS2 Directive was used as the initial analytical framework, as it represents the most precise and legally binding systematization of security requirements currently available under EU legislation. For each of the ten categories, the text of

the BiH Law on Personal Data Protection was examined using qualitative content analysis to identify provisions that substantively correspond to the given category, regardless of terminological differences between the two texts.

3.4 Coverage Assessment Scale

Each category was assigned a coverage-level score according to a three-point scale, adapted from the approach commonly used in practical NIS2 gap analyses [23] and broadly consistent with systematic requirements-mapping methodologies previously applied to GDPR-derived obligations in the requirements-engineering literature [11]:

- Fully covered: the law contains an explicit, concrete provision that essentially corresponds to the requirement of the given NIS2 category.
- Partially covered: the law contains a general or implicit provision that can be interpreted as covering the category, but without the technical specificity or operational detail required by NIS2/the Implementing Regulation.
- Not covered: the law contains no provision substantively related to the given category.

We carried out the assessment independently, then compared the results to verify consistency; we resolved disagreements through discussion until we reached consensus. Initial (pre-consensus) inter-coder agreement across the ten categories was 80% (8 of 10 categories), corresponding to a Cohen's kappa of $\kappa = 0.64$, indicating substantial agreement. Initial divergence occurred on two categories, K1 (risk-analysis policies and IS security) and K5 (security in system acquisition, development and maintenance), both of which were initially coded as "Fully covered" by one researcher, reflecting a general reading of Arts. 37 and 27, respectively. Following discussion, both categories were reclassified as "Partially covered," on the argument, grounded in professional information-security practice, that the corresponding provisions establish the relevant obligation in principle but do not specify the technical or procedural detail (e.g., a defined risk-assessment methodology for K1, or mandated secure-coding standards and vulnerability-management lifecycle protocols for K5) required for a category to be considered fully covered under NIS2 and its Implementing Regulation. This more conservative, consensus interpretation is reflected in the results reported in Table 1.

3.5 Limitations of the Methodological Approach

The methodology has several deliberate limitations, discussed in more detail in Section 5.3: the analysis is based on the textual, doctrinal interpretation of the law rather than its actual implementation in practice; the NIS2 categories, although specified by the Implementing Regulation, still leave room for interpretation; and, finally, the mapping reflects the current (2026) state of both legal frameworks, which remain subject to future amendment.

4 Results

4.1 Mapping Table: NIS2 Article 21 Categories against the BiH Law on Personal Data Protection (2025)

Table 1 presents the outcome of the mapping exercise described in Section 3, showing, for each of the ten NIS2 categories, the corresponding provisions identified in the BiH Law on Personal Data Protection and the assessed degree of coverage. Figure 1 visualizes the same results.

Table 1 Degree of coverage of NIS2 categories of measures under the BiH Law on Personal Data Protection

#	NIS2 Category (Art. 21)	Corresponding Provisions of the BiH Law	Coverage
K1	Risk analysis policies and IS security	Art. 37 (Data Protection Impact Assessment)	Partial
K2	Handling of security incidents	Arts. 35, 36 (Part Two); Arts. 86, 87 (Part Three)	Partial
K3	Business continuity and crisis management	Art. 34(1)(c); Art. 85(1)(i)	Partial
K4	Supply chain security	Art. 30 (Processor – contractual regulation)	Partial
K5	Security in system acquisition, development and maintenance	Art. 27 (Data protection by design and by default)	Partial
K6	Assessment of the effectiveness of risk-management measures	Art. 34(1)(d)	Full
K7	Cyber hygiene and training	Art. 41(1)(b) – task of the DPO	Partial
K8	Cryptography and encryption	Arts. 27, 34(1)(a), 36(3)(a), 85(1)	Full
K9	Human resources security and access control	Art. 85(1)(a, e, g) – competent authorities only	Partial
K10	MFA and secure communication		Not covered

4.2 Summary Coverage Statistics

Table 2 summarizes the distribution of coverage levels across the ten NIS2 categories. Only two categories are fully covered, seven are partially covered, and one category is not covered at all, as illustrated in Figure 2.

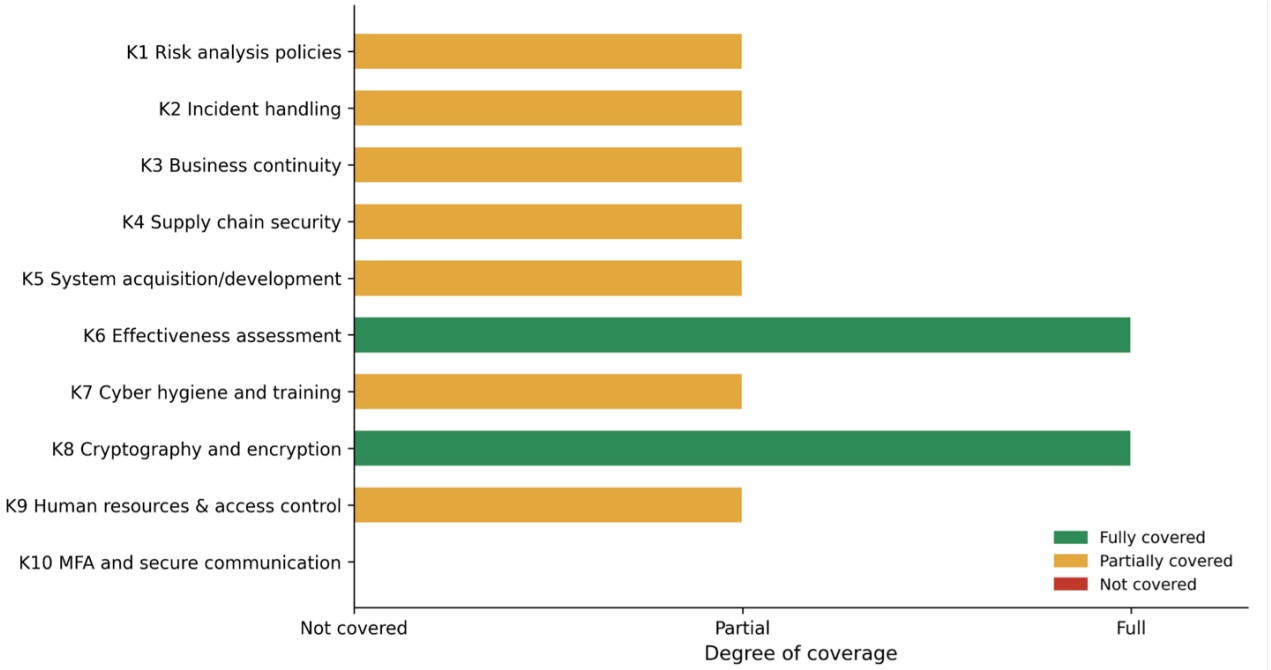


Figure 1 Degree of coverage of NIS2 categories of measures (Art. 21) under the BiH Law on Personal Data Protection (2025)

Table 2 Summary distribution of coverage levels

Coverage Level	Number of Categories	%
Fully covered	2	20%
Partially covered	7	70%
Not covered	1	10%

4.3 Key Findings

No category is entirely uncovered except K10 (MFA). The Law, although focused on personal data protection, nonetheless touches upon most NIS2 categories at least indirectly, confirming the previously cited ENISA finding of a high degree of conceptual overlap between GDPR-related frameworks and NIS2 requirements.

The dominant pattern is "partial coverage" (70% of categories): the Law establishes principles (e.g., regular testing of measures, availability recovery, data protection by design), but almost never descends to the technical operational level required by NIS2/the Implementing Regulation (concrete deadlines, concrete technical standards, formalized plans).

An interesting asymmetry exists between Part Two and Part Three of the Law: the provisions relating to processing by competent authorities in the criminal-law context (Art. 85) contain a significantly more precise and technically elaborated list of access-control and logging measures than the general provisions applicable to economic operators and public bodies (Art. 34). This is relevant because it is precisely economic operators (particularly in the energy, telecommunications, and digital sectors) that are the primary addressees of the NIS2 Directive, yet the Law regulates them under the most generic standard.

The largest gap (K10 – MFA) and the weakest-covered categories (K4 – supply chain security, K7 – cyber hygiene) represent exactly the dimensions most frequently exploited by contemporary attacks on critical infrastructure (compromised credentials, third-party attacks, human error), suggesting that future legislative interventions in BiH should prioritize precisely these areas. This concern is

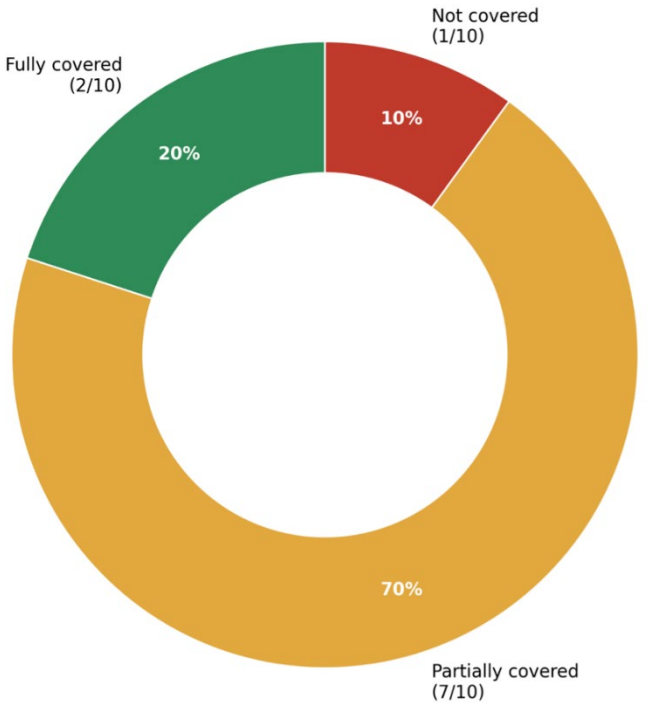


Figure 2 Summary distribution of coverage levels (10 NIS2 categories of measures)

reinforced by the wider cybersecurity literature, which identifies multi-factor authentication as one of the most effective and cost-efficient controls against unauthorized access and credential-based compromise, precisely the attack vector that a purely password- or single-factor-based access model leaves exposed [24].

5 Discussion

5.1 Interpretation of the Main Finding

The results of the comparative analysis show that the BiH Law on Personal Data Protection (2025), although clearly narrower in focus on protecting individuals' rights in relation to the processing of personal data, nonetheless conceptually covers nine of the ten categories of security measures prescribed by Article 21 of the NIS2 Directive at least partially. This finding confirms the previously cited ENISA conclusion [1] that GDPR-inspired data-protection frameworks and NIS2 share a core set of technical principles: confidentiality, integrity, availability, and regular testing of security measures.

However, the dominance of the “partially covered” category (70%) points to a pattern that is, for doctoral-level analysis, more significant than the raw figure itself: the Law consistently formulates principles but avoids technical operational elaboration. This is understandable given the nature and purpose of the Law; unlike the NIS2 Directive and its Implementing Regulation [6], it is a legal instrument focused on individual rights rather than a sectoral technical standard for system resilience.

5.2 Practical Implications

For organizations in BiH: The mapping results can serve as a practical reference point for organizations that, through regional initiatives or business relationships with EU partners, encounter NIS2-inspired expectations. Organizations should not misinterpret compliance with this Law as sufficient for broader cybersecurity resilience, particularly with regard to categories K4, K7, and K10. The weak coverage of K4 (supply chain security) is consistent with the broader direction of recent EU cybersecurity regulation, which increasingly imposes explicit supply-chain and coordinated vulnerability-disclosure obligations as illustrated by the Cyber Resilience Act's new requirements in this area [25] – and with the wider evolution of EU product-safety and cybersecurity law more generally [26], neither of which is yet mirrored in the BiH Law's data-protection provisions.

Enforcement intensity is a further dimension not captured directly by the present mapping but relevant to its practical implications. Comparative research on the enforcement mechanisms of NIS2, GDPR, and other data-security frameworks indicates that the credibility of a compliance regime depends heavily on the severity and diversity of the sanctions actually available and applied [27], while empirical analysis of GDPR enforcement fines shows that cybersecurity-related violations already rank among the more heavily sanctioned categories of infringement under that Regulation [28]. Because the BiH Law does not yet specify a comparably calibrated sanctioning regime for the technical measures examined in this paper, the practical deterrent effect of the categories assessed as "partially covered" remains an open empirical question for future research.

For regulators and policymakers: The finding of a pronounced asymmetry between the technical precision of the provisions for competent authorities (Art. 85) and the generic provisions for economic operators (Art. 34) raises a concrete policy question: if the legislator was willing to precisely and technically elaborate access-control and logging measures for processing in the context of criminal prosecution, there is no obvious obstacle to applying similar technical precision to economic operators through the secondary legislation envisaged under Article 117 of the Law.

For the DPO profession/community: The finding that employee training (K7) is regulated exclusively as a task of the data protection officer suggests that data protection officers in BiH may have an opportunity to extend their mandate toward cyber-hygiene practices, thereby partially bridging this gap even before any potential legislative intervention.

5.3 Research Limitations

This research has several methodological limitations: (1) its doctrinal, non-empirical nature the analysis relies exclusively on the text of the law rather than its actual implementation in practice; (2) the subjectivity inherent in qualitative assessment, although dual independent coding was applied; (3) an asymmetry in the sources used for the NIS2 side of the mapping, since some categories were further specified using secondary sources; (4) the temporal limitation of the findings, given that secondary legislation is still under preparation; and (5) the focus on a single national context, although the methodology applied in this paper can serve as a replicable framework for similar research in the region.

5.4 Connection to the Broader Regional Context

The findings of this paper are complementary to earlier cybersecurity research in the Western Balkans region. Kepuska and Tomasevic [16] identified a similar pattern in the context of higher-education institutions: the existence of basic security principles alongside a lack of operationally elaborated plans and procedures. The results of this study suggest that this pattern is likely more broadly present in the regulatory architecture of Western Balkan countries, opening space for a wider, comparative regional study.

6 Conclusion

This paper systematically mapped the technical and organizational measures prescribed by the new Law on Personal Data Protection of Bosnia and Herzegovina (2025) against the ten categories of security measures prescribed by Article 21 of the EU NIS2 Directive. The analysis showed that the Law conceptually addresses nine of the ten examined categories, with a dominant pattern of partial coverage (70% of categories). Only two categories are fully covered: cryptography/encryption and the assessment of the effectiveness of security measures, while the category of multi-factor authentication remains entirely uncovered. A key finding of this paper is the asymmetry within the Law itself between the provisions applicable to competent authorities in the criminal-law context and those applicable to economic operators and public bodies.

Based on these findings, the answer to the paper's research question is as follows: the technical and organizational measures prescribed by the BiH Law on Personal Data Protection cover a broad, but shallow, portion of the NIS2 Directive's requirements, sufficient as a conceptual foundation, but insufficient as a stand-alone basis for compliance with the expectations of systemic cybersecurity resilience for critical infrastructure.

6.1 Recommendations

- For the legislature and the Personal Data Protection Agency: use the deadline for adopting secondary legislation (Art. 117) as an opportunity to technically specify the content of “appropriate technical and organizational measures,” following the example of Art. 85.
- For sectoral policymakers: consider developing a dedicated, sector-specific legal framework for the cybersecurity of critical infrastructure.
- For organizations: use the mapping table presented in this paper as an initial reference point for self-assessing remaining gaps.
- For the academic community: replicate the proposed mapping methodology in other Western Balkan countries.

6.2 Directions for Future Research

This paper is conceived as the first, foundational phase of a broader research program, which opens space for further development in the following directions: an empirical assessment of the implementation of the identified measures in organizations in Bosnia and Herzegovina; monitoring of the secondary legislation envisaged under Article 117 of the Law; a comparative regional study extending the methodology to other Western Balkan countries; and the development of a practical governance framework to help organizations in BiH align their security policies with the GDPR, NIS2, and related regulations. These directions form the foundation for the authors' further doctoral research in cybersecurity governance, regulatory compliance,

and information-system governance, with a focus on Bosnia and Herzegovina and the Western Balkans.

Conflicts of Interest: The authors report there are no competing interests to declare.

Data availability statement: The data presented in this study are available on request from the corresponding author.

References

[1] European Union Agency for Cybersecurity (ENISA), "Supporting NIS2 Implementation Through Actionable Guidance-Technical Implementation Guidance on Cybersecurity Risk Management Measures," 2025. [Online]. Available: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[2] International Association of Privacy Professionals (IAPP), "NIS2 Directive: Mapping the Interplays with the GDPR," 2026. [Online]. Available: https://iapp.org/resources/article/mapping-interplays-gdpr-nis2 . [Accessed: 17-Aug-2026].

[3] European Parliament and Council, "Regulation (EU) 2016/679 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 (General Data Protection Regulation)," Official Journal of the European Union, OJ L 119, pp. 1-88, 4 May 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] K. Hjerppe, J. Ruohonen, and V. Leppanen, "The General Data Protection Regulation: Requirements, Architectures, and Constraints," in *2019 IEEE 27th International Requirements Engineering Conference (RE)*, Jeju Island, Korea (South): IEEE, Sep. 2019, pp. 265–275. doi: 10.1109/RE.2019.00036.

[5] European Parliament and Council, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," Official Journal of the European Union, OJ L 333, pp. 80-152, 27 Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[6] European Commission, "Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures," Official Journal of the European Union, 7 Nov. 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

[7] M. Kianpour, P. A. Earls Davis, and I. M. Windekilde, "Digital sovereignty in practice: analyzing the EU's NIS2 directive," *Int. J. Inf. Secur.*, vol. 24, no. 4, p. 167, Aug. 2025, doi: 10.1007/s10207-025-01090-4.

[8] J. Ruohonen, "A Systematic Literature Review on the NIS2 Directive," arXiv preprint, arXiv:2412.08084, Dec. 2024. [Online]. Available: https://arxiv.org/abs/2412.08084

[9] D. Shamatonova, "The importance of the NIS2 Directive and the potential challenges it entails," *JARSSH*, vol. 11, no. 1, pp. 46–48, Mar. 2025, doi: 10.61841/7k8bwj71.

[10] J. Ruohonen, K. Hjerppe, and E.-Y. Kang, "A Mapping Analysis of Requirements Between the CRA and the GDPR," in *2025 IEEE 33rd International Requirements Engineering Conference Workshops (REW)*, Valencia, Spain: IEEE, Sep. 2025, pp. 215–222. doi: 10.1109/REW66121.2025.00034.

[11] C. Negri-Ribalta, M. Lombard-Platet, and C. Salinesi, "Understanding the GDPR from a requirements engineering perspective—a systematic mapping study on regulatory data protection requirements," *Requirements Eng*, vol. 29, no. 4, pp. 523–549, Dec. 2024, doi: 10.1007/s00766-024-00423-4.

[12] United Nations Development Programme (UNDP) Slovakia, "Cybersecurity for a Resilient Digital Future," 2025. [Online]. Available: https://publicfinance.undp.sk/en/regional-project-cybersecurity/ . [Accessed: 17-Aug-2026].

[13] "Global Cyber Policy Dialogues: Western Balkans," Meeting Summary, Observer Research Foundation (ORF) America, Apr. 2026. [Online]. Available: https://orfamerica.org/recent-events/global-cyber-policy-dialogues-western-balkans-montenegro . [Accessed: 17-Aug-2026].

[14] European Commission, "NIS2 Directive: securing network and information systems," Shaping Europe's Digital Future, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive [Accessed: 17-Aug-2026].

[15] European Cyber Security Organisation (ECSO), "NIS2 Directive Transposition Tracker," 2026.

[16] K. Kepuska and M. Tomasevic, "A lightweight framework for cyber risk management in Western Balkan higher education institutions," *PeerJ Computer Science*, vol. 10, p. e1958, Apr. 2024, doi: 10.7717/peerj-cs.1958.

[17] L. Puljak, A. Mladinić, R. Iphofen, and Z. Koporc, "Before and after enforcement of GDPR: Personal data protection requests received by Croatian Personal Data Protection Agency from academic and research institutions," *Biochem. med. (Online)*, vol. 30, no. 3, pp. 363–370, Oct. 2020, doi: 10.11613/BM.2020.030201.

[18] D. Mellafe Z., "The Coverage Gap: Chile's Cyber Disclosure Framework versus the USA, EU and UK," arXiv preprint, arXiv:2606.05594, Jun. 2026. [Online]. Available: https://arxiv.org/abs/2606.05594

[19] Parliamentary Assembly of Bosnia and Herzegovina, "Law on Personal Data Protection," Official Gazette of BiH, no. 12/25, 28 Feb. 2025. [Online]. Available: https://www.sluzbenilist.ba/page/akt/aCRNh0ohz4nh78h77P7BE=

[20] CMS Legal Services EEIG, "Data protection and cybersecurity laws in Bosnia and Herzegovina," CMS Expert Guide to Data Protection and Cyber Security Laws, 2025. [Online]. Available: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/bosnia-and-herzegovina [Accessed: 17-Aug-2026].

[21] CEE Legal Matters / Lexology, "New Personal Data Protection Law Enters Into Force in Bosnia and Herzegovina," Nov. 2025. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=27daf304-9c5b-4c79-a8bb-c6e861fbc1af . [Accessed: 17-Aug-2026].

[22] M. Seeba, M. Valgre, and R. Matulevičius, "Evaluating Organization Security: User Stories of European Union NIS2 Directive," in *Advanced Information Systems Engineering*, vol. 15701, J. Krogstie, S. Rinderle-Ma, G. Kappel, and H. A. Proper, Eds., Cham: Springer Nature Switzerland, 2025, pp. 57–74. doi: 10.1007/978-3-031-94569-4_4.

[23] NIS2-Templates.com, "Your NIS2 Gap Analysis in 5 Phases," 2026. [Online]. Available: https://www.nis-2-templates.com/gap-analysis/ . [Accessed: 17-Aug-2026].

[24] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure," *Future Internet*, vol. 15, no. 4, p. 146, Apr. 2023, doi: 10.3390/fi15040146.

[25] J. Ruohonen and P. Timmers, "Vulnerability Coordination under the Cyber Resilience Act," *Applied Cybersecurity & Internet Governance*, Nov. 2025, doi: 10.60097/ACIG/213350.

[26] J. Ruohonen, "A review of product safety regulations in the European Union," *Int. Cybersecur. Law Rev.*, vol. 3, no. 2, pp. 345–366, Dec. 2022, doi: 10.1365/s43439-022-00057-8.

[27] S. Park and J. D. Hastings, "Weak Enforcement and Low Compliance in PCI DSS: A Comparative Security Study," in *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, Boston, MA, USA: IEEE, Mar. 2026, pp. 1–6. doi: 10.1109/ISDFS69419.2026.11458981.

[28] J. Ruohonen and K. Hjerppe, "The GDPR enforcement fines at glance," *Information Systems*, vol. 106, p. 101876, May 2022, doi: 10.1016/j.is.2021.101876.