

The step under review	Adopt and implement cybersecurity legislative framework that is fully aligned with EU cybersecurity policy and EU cybersecurity acquis, i.e. the Law on security of networks and information systems and updated cybersecurity strategy.
Baseline	(2024) is 0
Deadline of the step	June 2025
Actual results	<p>The legislative process was initiated several years ago under the previous government, which pursued a different conceptual approach to alignment with the directive. Building on that initial effort, two public versions of the draft law were prepared and published on the national consultation portal ENER: the first on 18 December 2024 and the second on 29 January 2025 (links are provided below). Both versions were made available for stakeholder input and public comment.</p> <p>A Multisectoral Working Group was established by the Ministry of Digital Transformation on 30 August 2024, composed of representatives from 19 institutions. The group held a series of technical meetings and bilateral consultations, where specific provisions were reviewed in detail to ensure clarity, institutional feasibility, and consistency with the country's legal framework. The Ministry also organized a public hearing on the draft law on 7 March 2025, following which the revised draft was resubmitted to the same 19 institutions for final review. A second public hearing was later held in the Parliament as part of the adoption procedure.</p> <p>Given that cybersecurity was previously unregulated in the national legal system, a formal GAP analysis was not conducted. Instead, a suite of supporting analytical documents was prepared to accompany the legislative proposal. These include a report on the level of transposition of the NIS2 Directive in the current draft law (annex 5), a legal compliance report (annex 7), and a comparative analysis of salaries between the public and private sectors (Annex 6) to inform future human resource policies in the field of cybersecurity. An additional institutional structure analysis (annex 8) was also developed, examining existing administrative mandates and proposing recommendations for the new institutional arrangements to be formalized under the law.</p> <p>In parallel, a Regulatory Impact Assessment (Annex 3) was carried out to assess the potential legal, financial and administrative effects of the law. The legislative package also includes a Table of Concordance (Annex 4) mapping national provisions against the NIS2 Directive, with explanations of how each</p>

provision aligns with EU requirements, and a **formal Compliance Statement (Annex 4d) and Conformation Statement (Annex 4e)** of alignment.

The draft law was first submitted to the **EU Delegation (EUD)** on **20 March 2025**, and a revised version was shared on **16 April 2025** following feedback from stakeholders and internal reviews. Comments from the **European Commission** were received shortly before parliamentary adoption, and the same are widely addressed and explained in the **Explanatory note and final concordance table (Annex 4b and 4c)**. The law was adopted as a strategic legislative package by the **Government on 27 May 2025** and subsequently adopted by the **Parliament on 27 June 2025**. It was published in **Official Gazette No. 135 on 4 July 2025 (Annex 2)**.

All relevant supporting documents, including the draft law, RIA, technical analyses, compliance statement, table of concordance, and records of public consultations, are included in the final legislative dossier.

Cybersecurity Strategy

The National Cybersecurity Strategy (2025–2028)¹ of the Republic of North Macedonia is a strategic document aimed at ensuring a secure, resilient, and trustworthy digital environment through a range of activities and measures. Its goal is to make North Macedonia a safe place for online operations and work, supported by advanced human and technical capacities. The core premise of the National Cybersecurity Strategy is to establish conditions for a coordinated national response to cybersecurity challenges, as well as to prevent cyber incidents and attacks through the development of resilient digital infrastructure and human capabilities.

To prepare the Cybersecurity Strategy 2025–2028, along with the Action Plan, an inter-institutional Working Group was established, led by the Ministry of Digital Transformation. The Working Group was officially formed by a decision dated August 30, 2024. It consists of representatives from the following institutions: Ministry of Digital Transformation, Ministry of Internal Affairs, Ministry of Foreign Affairs and Foreign Trade, Ministry of Defence, UGD Military Academy – Skopje, Agency for Electronic Communications and MKD-CIRT, National Security Agency, Personal Data Protection Agency, Operational-Technical Agency – Skopje, Directorate for Security of Classified Information, Intelligence Agency, “Goce Delchev” University – Shtip, and the State Audit Office.

The Working Group held several working meetings. The draft Strategy was published on ENER (Single National Electronic Registry) on October 15, 2024. A public debate at the Government was held on November 1, 2024. The first Information Note to the Government regarding the Cybersecurity Strategy

¹ <https://mdt.gov.mk/mk-MK/regulativa/strategija-za-sajber-bezbednost>

	<p>2025–2028 and the Action Plan was submitted on December 10, 2024, with the final revision made on January 16, 2025. Throughout the preparation process, a total of 86 comments were addressed. The same was adopted on 21.01.2025.</p>
<p>Evidence provided</p>	<p><u>Evidence related to the Law on security of networks and information systems:</u></p> <p>Annex 1: Government decision approving the text of the law</p> <p>Annex 2: Official Gazette of the Republic of North Macedonia No. 135/2025, published on 04.07.2025, confirming adoption of the Law on Security of Networks and Information Systems by the Parliament on 27.06.2025. The law enters into force on the eighth day following its publication in the Official Gazette and will apply as of 1 January 2026.</p> <p>Annex 2a Law on Security of Networks and Information Systems_EN</p> <p>Annex 3: Regulatory Impact Assessment</p> <p>Annexes 4 and 4a: Concordance tables (EU-MK, MK-EU)</p> <p>Annex 4b: Concordance table with feedback on comments received by the EC</p> <p>Annex 4c: Explanatory note</p> <p>Annex 4d: Compliance statement</p> <p>Annex 4e: Compliance statement assessment and conformation from the Secretariat for Legislation</p> <p>Annex 5: Report on level of transposition of the NIS 2 Directive into the draft text of the Law on Security of Networks and Information Systems</p> <p>Annex 6: Comparative analysis of salaries in the private sector and salaries in SABS</p> <p>Annex 7: Report on the compliance of the draft Law on Security of Networks and Information Systems with the existing legislation</p> <p>Annex 8 Report on the latest institutional structure envisaged by the LOOSAB</p> <p>Links to ENER of the publication from 2024² and 2023³</p> <p><u>Evidence related to the Cybersecurity Strategy 2025–2028</u></p> <p>Annex 9 Government decision approving the Cybersecurity Strategy and Action Plan, dated 21.01.2025</p> <p>Annex 10: decision for establishing working group</p>

² https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=88201

³ https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=80751

	Final Strategy text, published online ⁴ by the Ministry of Digital Transformation, ENER consultation link ⁵
Checks performed in the verification of the step and related findings	<p>A thorough verification process was conducted to ensure the alignment of the newly adopted Law on the Security of Network and Information Systems with the NIS 2 Directive. In the first place, this has been done with the Report on level of transposition of the NIS 2 Directive into the draft text of the Law on Security of Networks and Information Systems (Annex 5) and Report on the compliance of the draft Law on Security of Networks and Information Systems with the existing legislation (Annex 7). Then, this included a detailed, article-by-article review of the Table of Concordance, carried out jointly with the Secretariat for Legislation, ensuring that all legal gaps identified during the preparatory phase were adequately addressed and transposed. The legislative process followed a transparent and participatory approach, involving a public consultation via the ENER platform, as well as 2 public hearings. A comprehensive Regulatory Impact Assessment (RIA) was developed, analysing the legal, technical, and institutional implications of the law. Finally, a formal Declaration of Compliance was issued, confirming that the law aligns with the relevant provisions of the NIS 2 Directive. Four different documents (listed above) were prepared to ensure high quality and implementable legal framework.</p>
Compliance with general principles and DNSH principle	<p>The Law on the Security of Network and Information Systems fully complies with the general principles of transparency, accountability, evidence-based policymaking, and stakeholder participation, as well as the DNSH principle. It aligns with Directive (EU) 2022/2555 (NIS2), contributing to a more secure and resilient digital ecosystem in line with EU digital objectives.</p> <p>The legislative process was inclusive and transparent. Two public drafts were published on ENER (18 Dec 2024 and 29 Jan 2025), followed by a public hearing (7 Mar 2025) and a second hearing in Parliament. A Multisectoral Working Group with 19 institutions led technical consultations to ensure legal clarity and institutional feasibility. A Regulatory Impact Assessment and supporting analyses (including transposition reports, legal compliance, and institutional structure reviews) ensured alignment with EU law and national policy.</p> <p>Although a formal GAP analysis was not applicable due to the previously unregulated area, all relevant compliance and concordance documents were prepared and included in the legislative dossier. Feedback from the EU</p>

⁴ <https://mdt.gov.mk/mk-MK/regulativa/strategija-za-sajber-bezbednost>

⁵ <https://ener.gov.mk/Default.aspx?item=newdocumentdetails&detalisId=74>

	<p>Delegation and European Commission was integrated into the final draft, adopted by Parliament on 27 June 2025.</p> <p>The DNSH principle is respected through measures that promote digitalisation, reduce administrative burden, and support long-term sustainability by strengthening cybersecurity resilience and institutional efficiency.</p>
Double funding	Contributions from third parties were not reported in support of the achievement of this step.
Clear conclusion on the achievement of the step	Fully achieved