INSIGHT REGULATION & COMPLIANCE

Does NIS2 require post-quantum cryptography?

Not by name. NIS2 requires a cryptography policy that follows the state of the art, and the state of the art is moving away from quantum-vulnerable algorithms.



Sokaïna Jabbar
CEO, Co-Founder · Executive MBA
Reviewed by Carlos E. Avimadjessi

PUBLISHED	LAST REVIEWED	READING TIME
24 November 2026	24 November 2026	4 min

SHORT ANSWER

Not by name: neither the NIS2 Directive nor the Belgian NIS2 law mentions quantum computers. But NIS2 requires policies on the use of cryptography, and measures that take the state of the art into account. With the EU and NIST now setting end dates for quantum-vulnerable algorithms, a credible cryptography policy has to include a plan to replace them.

© 2026 Sorlos

Why the question comes up now

The Belgian NIS2 law of 26 April 2024 has applied since 18 October 2024, and the Centre for Cybersecurity Belgium (CCB) is now assessing how entities comply. At the same time, the EU's roadmap for post-quantum cryptography sets its first milestone at the end of 2026. The roadmap itself makes the link: it says its first steps "support the compliance with cybersecurity regulations, in particular the NIS2 Directive".

> NOTE
>
> This article is information, not legal advice. Whether an obligation applies to you depends on your sector, your size and the services you provide.

What NIS2 says about cryptography

Article 21 of the directive lists the minimum cybersecurity measures that essential and important entities must take. Point (h) requires "policies and procedures regarding the use of cryptography and, where appropriate, encryption". Article 21(1) adds that the measures must take into account "the state-of-the-art and, where applicable, relevant European and international standards", as well as the cost of implementation.

For some digital providers, the rules are more detailed. Implementing Regulation (EU) 2024/2690 applies to DNS service providers, cloud and data centre providers, managed service providers, managed security service providers and a few other digital services. Point 9 of its annex requires their cryptography policy to set:

What Implementing Regulation 2024/2690 asks of a cryptography policy

POINT	REQUIREMENT
9.2 (a)	The type, strength and quality of the cryptographic measures needed, according to how the assets are classified
9.2 (b)	The protocols and algorithms approved for use, "following, where appropriate, a cryptographic agility approach"
9.2 (c)	The approach to key management, from generating keys to destroying them
9.3	A review at planned intervals, "taking into account the state of the art in cryptography"

In Belgium, the CCB advises NIS2 entities to use its CyberFundamentals (CyFun) framework. A validated implementation gives a presumption of conformity with the risk-management measures.

Why the state of the art now includes post-quantum cryptography

NIS2 does not set a quantum deadline. The texts it refers to are what is changing.

- **The EU roadmap** asks for high-risk use cases to move to post-quantum cryptography "as soon as possible, no later than the end of 2030", and for as many systems as feasible by 2035.
- **NIST**, whose standards most products follow, confirmed in October 2026 that it "will deprecate quantum-vulnerable public-key cryptography after 2030 and disallow its use under NIST standards and guidelines after 2035". This covers RSA and elliptic-curve cryptography, whatever the key size.

A cryptography policy reviewed "taking into account the state of the art" cannot ignore these dates for long. The question a supervisor can reasonably ask is not whether you already use post-quantum algorithms, but whether you know where your quantum-vulnerable cryptography is and have a plan to replace it.

What it means for your organisation

1. **Check whether you are in scope.** In Belgium, an organisation is in principle covered if it provides a service listed in the annexes of the law, is established in Belgium and is at least a medium-sized enterprise. Some services are covered whatever their size. The CCB publishes a scope test.
2. **Reread your cryptography policy.** Check that it names the approved algorithms, says how they will be replaced, and has a review date. If it says nothing about quantum-vulnerable algorithms, that is the first gap to close.
3. **Add the quantum threat to your risk analysis.** The EU roadmap asks organisations to include it in their top-level risk management, so that it is discussed at board level.
4. **Start your cryptographic inventory.** You cannot plan a replacement without knowing what to replace. Our article What is a cryptographic inventory, and where do you start? explains how.
5. **Ask your suppliers.** NIS2 also covers supply chain security. Ask your critical suppliers what their post-quantum plan is, and when.

Sources

1. European Parliament and Council of the EU, Directive (EU) 2022/2555 (NIS2 Directive), Article 21, 14 December 2022.
https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

2. European Commission, Implementing Regulation (EU) 2024/2690 on cybersecurity risk-management measures, Annex, point 9 (Cryptography), 17 October 2024.
https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
3. Centre for Cybersecurity Belgium, The NIS2 Law (Law of 26 April 2024), 26 April 2024.
https://atwork.safeonweb.be/nis2
4. NIS Cooperation Group, EU PQC Workstream, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (Part 1, version 1.1), 23 June 2025.
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
5. National Institute of Standards and Technology (US), Transition to Post-Quantum Cryptography Standards (NIST IR 8547), 27 October 2026.
https://csrc.nist.gov/pubs/ir/8547/final

AI tools assisted with the research, drafting and fact-checking of this article. The author wrote and approved the final text, and a second reviewer checked every source against the original.

Need assistance for your transition?

Sorlos runs quantum readiness assessments. We assess your risk from your cryptographic inventory and design a migration roadmap you can rely on. Vendor-independent, from Brussels.

Talk to us · www.sorlos.eu/#contact



Sokaïna Jabbar

ICT and emerging Technology leader with 12+ years in operational management, innovation, tech strategy, and intra/entrepreneurship.

This PDF reproduces the article as of 24 November 2026. The online version, kept up to date, is at https://www.sorlos.eu/insights/does-nis2-require-post-quantum-cryptography/. © 2026 Sorlos. All rights reserved.