ICTRECHT

CHEAT SHEET

NIS2

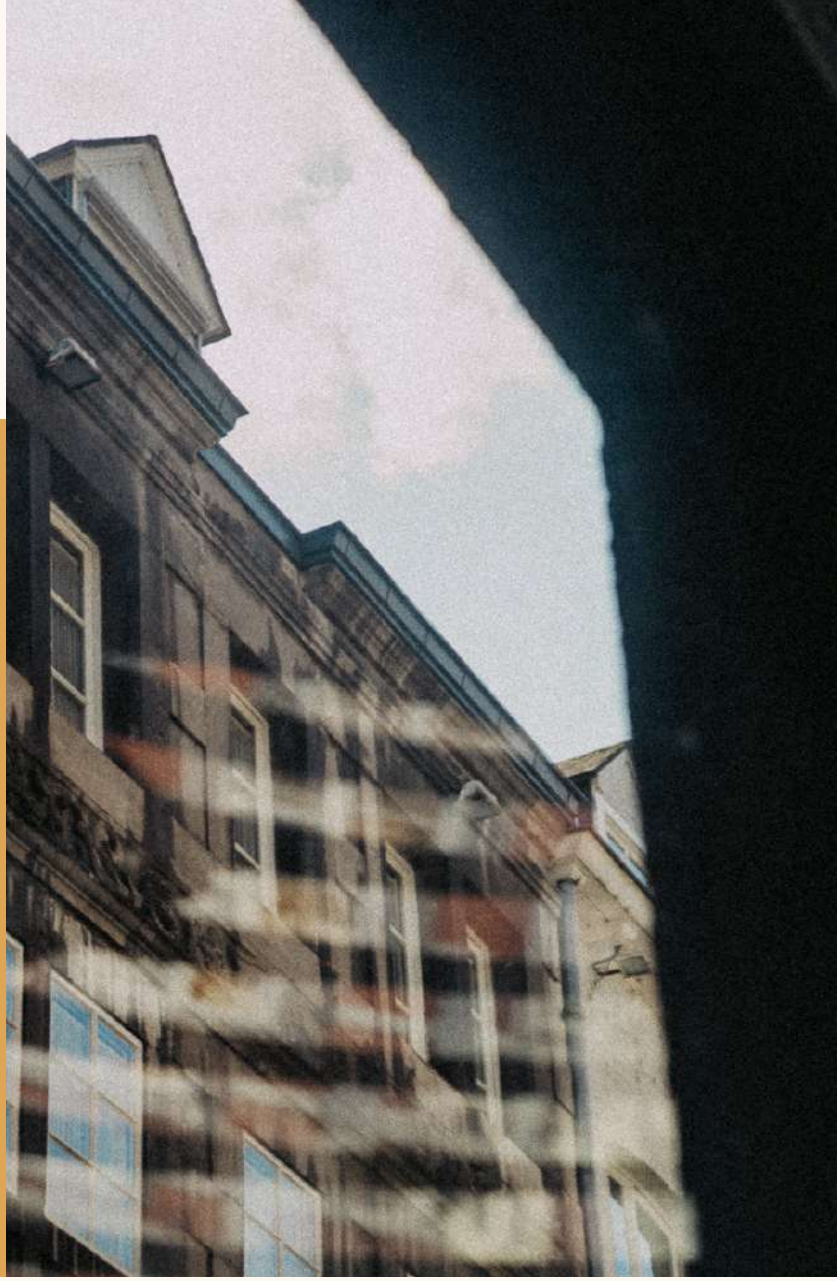
Get up to speed on the new rules in one minute.

Read more

Scope

Objective of NIS2

Ensuring and increasing cyber resilience



Who does it apply to?

Highly critical sectors Annex I - NIS2

Energy; transport; banking; financial market infrastructure; healthcare; drinking water; wastewater; digital infrastructure; ICT service management (business-to-business); government and space.

Other critical sectors Annex II - NIS2

Postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers and research.

An “essential” or “important” entity.

An entity is considered essential if it:

- Is active in a sector listed in Annex I to NIS2; an
- Is a “large” organisation, meaning it employs 250 people or more, or has an annual turnover exceeding EUR 50 million and a balance sheet total

Exception: The size criteria do not apply to parties such as providers of public electronic communications networks, DNS service providers, providers considered critical or presenting systemic risks, and central government authorities.

An entity is considered important if it:

- Is active in a sector listed in Annex I to NIS2; and
- Is a medium-sized organisation, meaning it employs fewer than 250 people and has an annual turnover not exceeding EUR 50 million, or an annual balance sheet total not exceeding EUR 43 million; or
- Is active in a sector listed in Annex II to NIS2; and
- Qualifies as a “large” or “medium-sized” organisation based on the above criteria.

Exception: If an undertaking employs fewer than 50 people and, in addition, has an annual turnover or annual balance sheet total below EUR 10 million, it is not considered a medium-sized undertaking.

3+1 obligations

01 Registration obligation

Entities must register with the competent authority, including Chamber of Commerce details and IP

02 Notification obligation

Notification to the CSIRT or the competent authority within 24 hours if there is a suspicion of a significant incident.

Within 72 hours, a report containing the initial assessment of the incident, its severity and impact, and, where possible, the indicators of compromise.

No later than one month after notification and resolution of the incident, a final report containing, among other things, a detailed description of the cause, the risk mitigation measures applied and ongoing, and the impact of the incident.

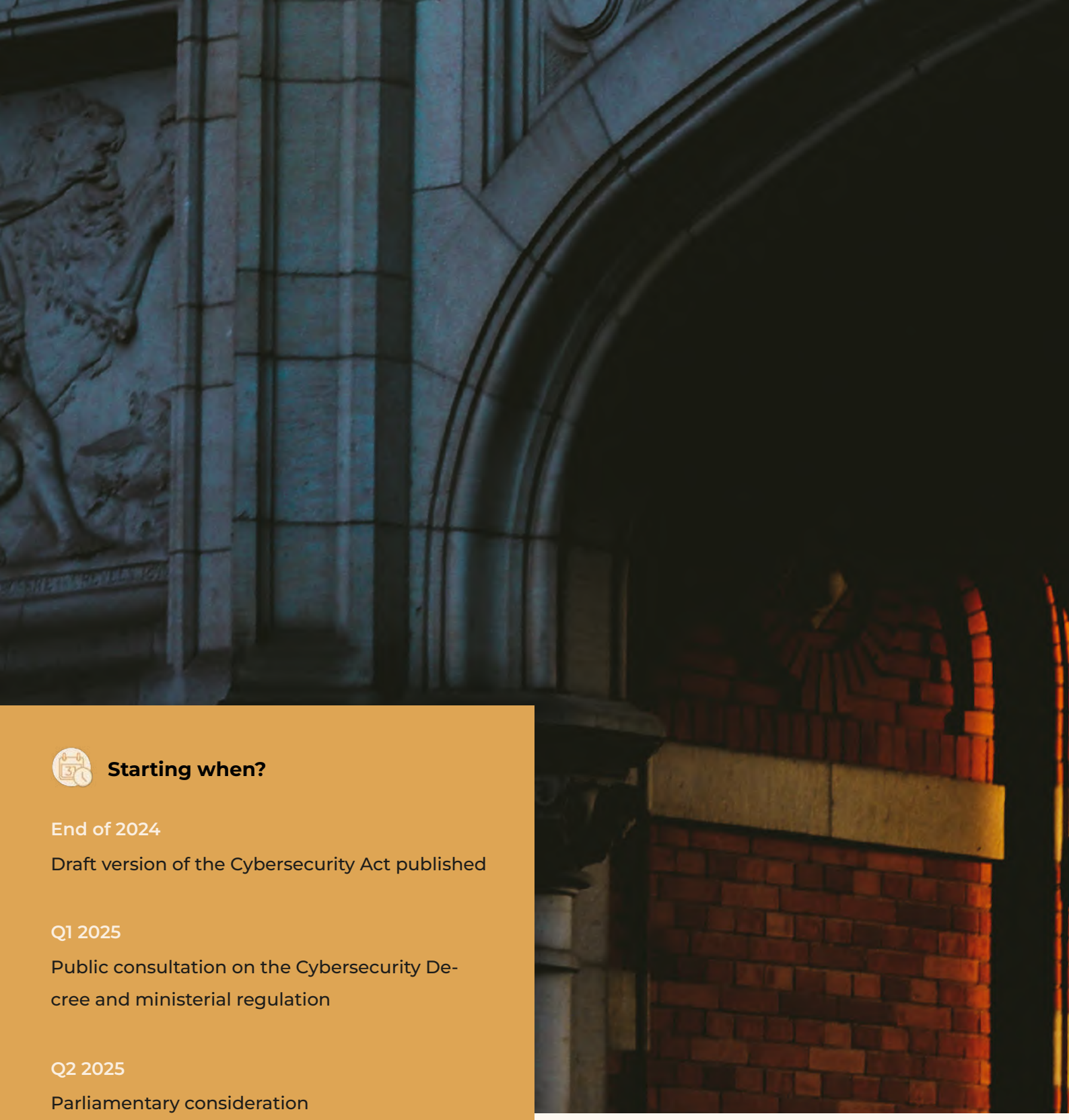
03 Duty of care

Measures for managing cybersecurity risks, such as:

- Risk analyses
- Incident handling
- Business continuity
- Supply chain security
- Security in the acquisition, development and maintenance of network and information systems
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies on the use of cryptography and encryption
- Personnel security aspects, access control policies and asset management
- Where appropriate, the use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications, and secure emergency communication systems within the organisation

+1 Governance

Directors must be more involved in the cybersecurity of their organisation and may also be held accountable. Directors must pay attention to their level of cybersecurity knowledge by following appropriate training.



Starting when?

End of 2024

Draft version of the Cybersecurity Act published

Q1 2025

Public consultation on the Cybersecurity Decree and ministerial regulation

Q2 2025

Parliamentary consideration

Q3 2025:

Cybersecurity Act enters into force

* The government has announced that it will not meet the official deadline. This is the expected timeline based on the information it has provided.

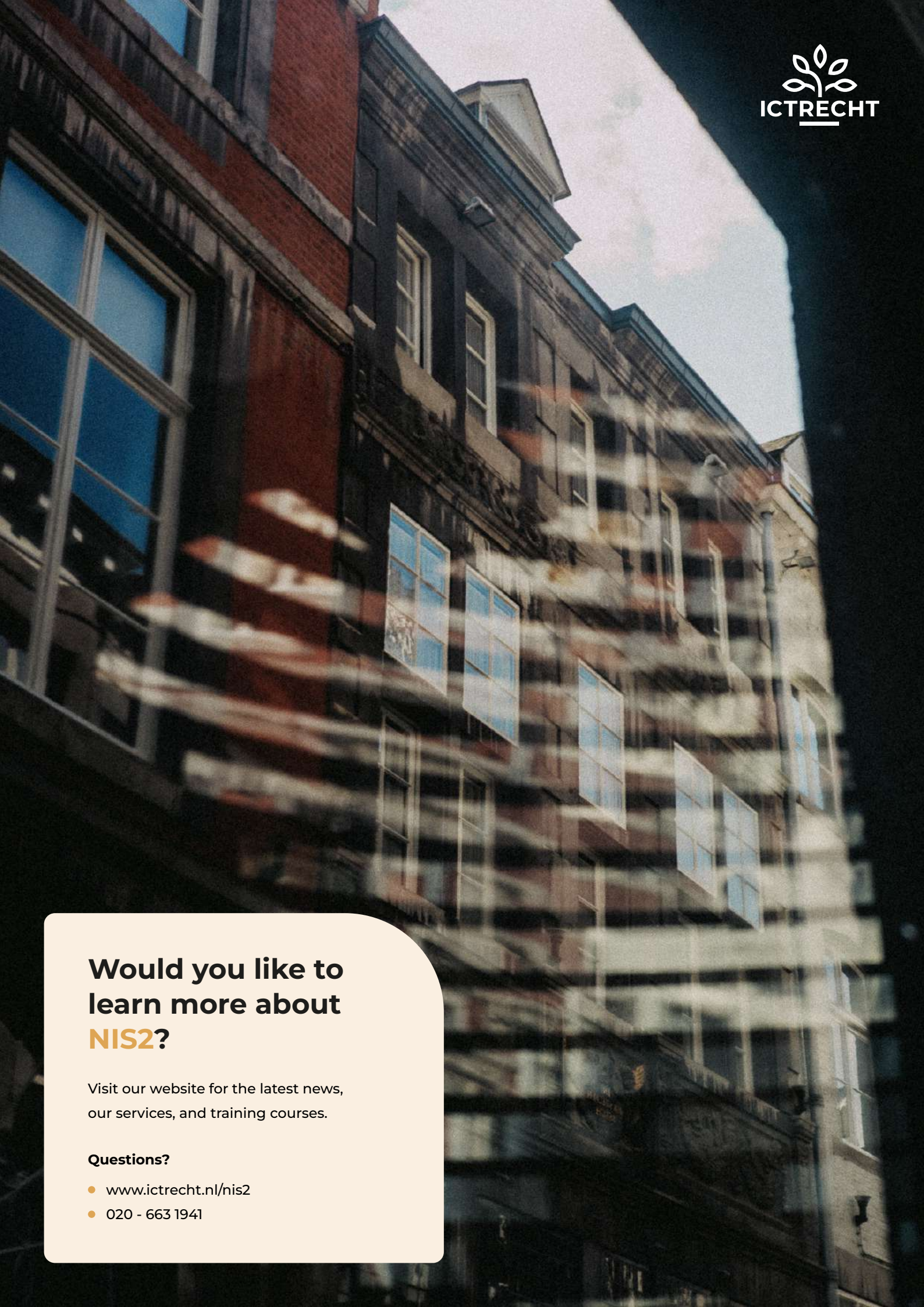
Sanctions

- **Essential entities**

  A possible fine of up to EUR 10 million, or 2% of annual turnover.

- **Important entities**

  A possible fine of up to EUR 7 million, or 1.4% of annual turnover.



ICTRECHT

Would you like to learn more about NIS2?

Visit our website for the latest news, our services, and training courses.

Questions?

- www.ictrecht.nl/nis2
- 020 - 663 1941