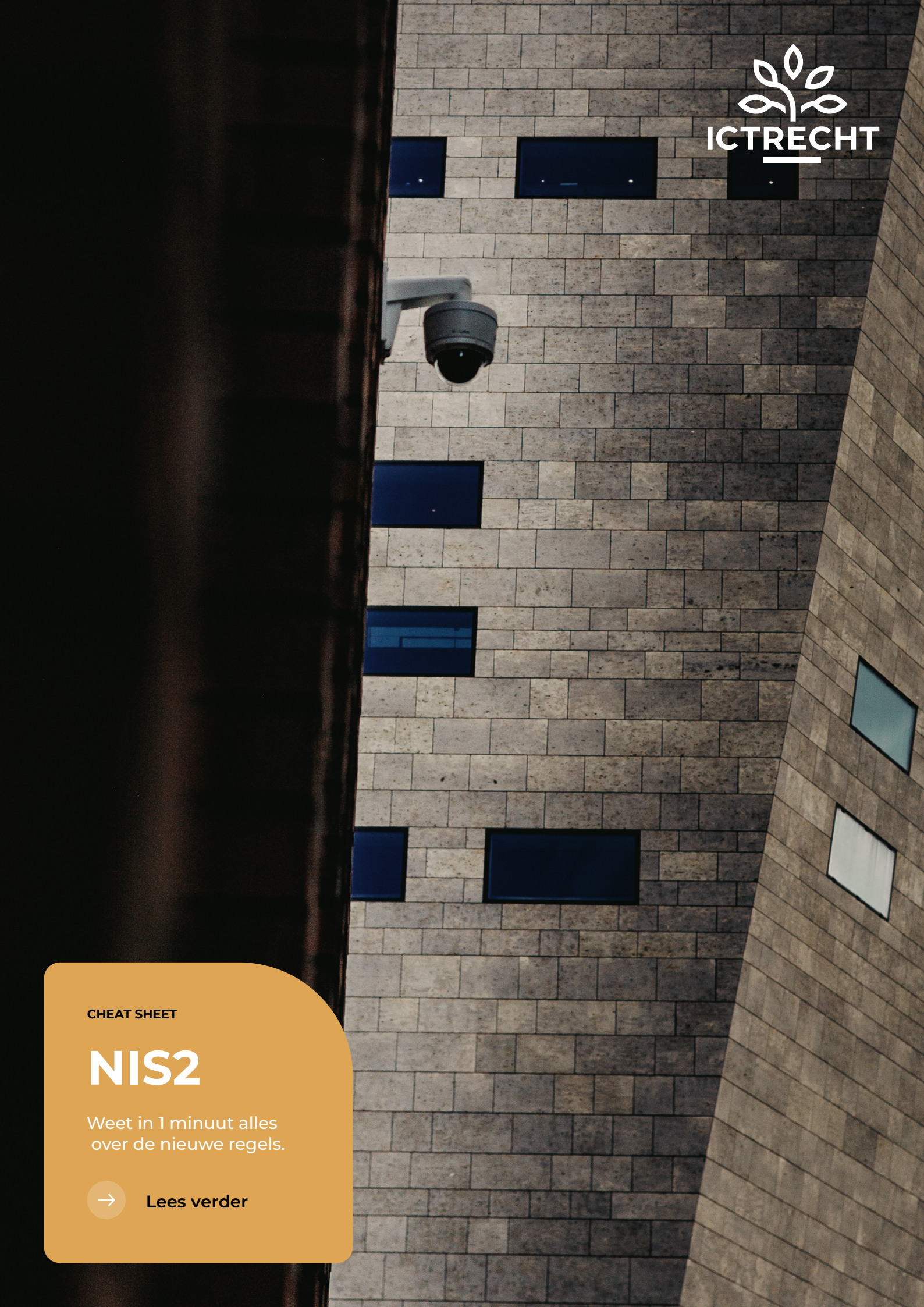

ICTRECHT

CHEAT SHEET

NIS2

Weet in 1 minuut alles over de nieuwe regels.

Lees verder

Scope

Doel van NIS2

Het waarborgen en verhogen van de cyberweerbaarheid

Voor wie?

- **Zeer kritieke sectoren**

Energie; vervoer; bankwezen; infrastructuur voor de financiële markt; gezondheidszorg;drinkwater; afvalwater; digitale infrastructuur; beheer van ICT-diensten (business-to-business); overheid en ruimtevaart.

Bijlage I NIS2

- **Andere kritieke sectoren**

Post- en koeriersdiensten; afvalstoffenbeheer; vervaardiging, productie en distributie van chemische stoffen; productie, verwerking en distributie van levensmiddelen; vervaardiging; digitale aanbieders en onderzoek.

Bijlage II NIS2

Een “essentiële” of “belangrijke” entiteit.

Een entiteit wordt als essentieel beschouwd wanneer deze:

- Actief is in een sector genoemd in Bijlage I van NIS2; en
- Een “grote” organisatie is van 250 personen of meer, of een jaaromzet heeft van meer dan €50 miljoen en een balanstotaal boven de €43 miljoen.

Uitzondering: De omvangcriteria zijn niet van toepassing op partijen zoals aanbieders van openbare elektronische communicatienetwerken, DNS-dienstverleners, aanbieders die als kritiek worden gezien of systeemrisico’s kennen en centrale overheidsinstanties.

Een entiteit wordt als belangrijk beschouwd wanneer deze:

- Actief is in een sector genoemd in Bijlage I van NIS2; en
- Middelgrote ondernemingen zijn ondernemingen waar minder dan 250 personen werkzaam zijn, en met een jaaromzet niet meer dan 50 miljoen euro, of een jaarlijks balanstotaal van niet meer dan 43 miljoen euro.
- Actief is in een sector genoemd in Bijlage II van NIS2; en
- Een “grote” of “middelgrote” organisatie is op basis van bovengenoemde criteria.

Uitzondering: Als er bij de onderneming minder dan 50 personen werkzaam zijn en als deze daarnaast een jaaromzet of jaarbalans heeft die lager is dan 10 miljoen euro, wordt deze niet gezien als middelgrote onderneming.

3 + 1 verplichtingen

01

Registratieplicht

Entiteiten moeten bij de bevoegde autoriteit o.a. KVK-gegevens, en IP-adressen registreren.

02

Meldplicht

Binnen 24 uur melden bij CSIRT of bevoegde autoriteit bij vermoeden van een significant incident.

Binnen 72 uur een rapportage met daarin de initiële beoordeling van het incident, de ernst en gevolgen ervan en, wanneer mogelijk, de signalen van aantasting.

Uiterlijk 1 maand na melding en beëindiging van het,incident een eindverslag met o.a. een grondige beschrijving van de oorzaak, de toegepaste en lopende risicobeperkende maatregelen en de gevolgen van het incident.

03

Zorgplicht

Maatregelen voor het beheer van cyber - beveiligingsrisico's, zoals

- Risicoanalyses
- Incidentenbehandeling
- Bedrijfscontinuïteit
- Beveiliging van de toeleveringsketen
- Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerken informatiesystemen
- Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen
- Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging
- Beleid inzake het gebruik van cryptografie en encryptie
- Beveiligingsaspecten voor personeel, toegangsbeleid en beheer van activa
- Wanneer gepast, gebruik van MFA of continueauthenticatieoplossingen, beveiligde spraak-, videoen tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de organisatie

Governance

Bestuurders moeten meer betrokken zijn bij cyberveiligheid van hun organisatie en kunnen ook verantwoordelijk gehouden worden. Bestuurders moeten aandacht besteden aan hun kennisniveau van cyberveiligheid door een opleiding te volgen.

Sancties

- **Essentiële entiteiten**

  een mogelijke boete van

  Maximaal €10 miljoen; of **2%** van de jaaromzet

- **Belangrijke entiteiten**

  een mogelijke boete van

  €7 miljoen; of **1,4%** van de jaaromzet

Vanaf wanneer?

Eind 2024:

Concept versie van de Cyber-beveiligingswet gepubliceerd

Q1 2025:

Internetconsultatie Cyber-beveiligingsbesluit en ministeriële regeling

Q2 2025:

Parlementaire behandeling

Q3 2025

Cyberbeveiligingswet wordt van kracht.

* De overheid heeft aangekondigd dat ze de officiële deadline niet gaan halen. Dit is de verwachte tijdslijn op basis van de informatie die zij heeft gegeven.

ICTRECHT

Wil je meer weten over de NIS2?

Bezoek onze website
voor het laatste nieuws,
onze diensten en trainingen.

Vragen?

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