GRATIS EXTRACT — CYBERBEVEILIGINGSWET (NIS2) STARTERKIT

Scope-zelfcheck: val ik onder de Cyberbeveiligingswet, of krijg ik ermee te maken als leverancier?

Een eerste, informele indicatie in 5–10 minuten — geen officieel beslisschema, geen automatische score (die staat in de volledige versie). Twijfelt u na het invullen? Check het officiële entiteitenregister via MijnNCSC (NCTV) of vraag een jurist.

Deel A — ben ik zelf een essentiële of belangrijke entiteit?

Zo nee op vraag 1: de rest van Deel A is waarschijnlijk niet van toepassing — ga naar Deel B.

1 Is uw organisatie actief in een van de 18 NIS2-sectoren (o.a. energie, vervoer, bankwezen, gezondheidszorg, digitale infrastructuur, overheid, afvalbeheer, chemie, voedsel)? ☐
Zo nee: ga direct naar Deel B.

2 Heeft uw organisatie ≥ 50 medewerkers én ≥ €10 miljoen jaaromzet of balanstotaal? ☐
De standaard-drempel voor middelgroot+; met uitzonderingen.

3 Bent u aanbieder van vertrouwensdiensten, TLD-naamregister, DNS-dienstverlener of andere partij die zonder omvangsdrempel altijd in scope is? ☐

4 Bent u een overheidsorganisatie (ministerie, gemeente boven de bestuurlijke drempel, provincie, waterschap)? ☐

5 Bent u eerder individueel aangewezen door de minister als essentiële/ belangrijke entiteit, ook zonder aan de standaarddrempels te voldoen? ☐

Deel B — ben ik leverancier van een entiteit die in scope is?

Voor de meeste MKB-bedrijven relevanter dan Deel A: u hoeft zelf niet in scope te zijn om toch beveiligingsvragen van een klant te krijgen.

1 Heeft u één of meer klanten die zelf onder de Cyberbeveiligingswet vallen (zie Deel A voor sector/omvang)? ☐

2 Heeft u ooit van een klant een beveiligings-/leveranciersvragenlijst, audit, of verzoek om een certificaat (ISO 27001, SOC 2, SC10) ontvangen? ☐

3 Levert u IT, software, hosting, consultancy of andere diensten die relevant zijn voor de informatiebeveiliging van een in-scope klant (ook een klein deel van uw omzet)? ☐

4 Verwacht u dat een bestaande klant u de komende 12 maanden zal vragen om aantoonbare basismaatregelen (MFA, patchbeleid, incidentmelding, training)? ☐

Meerdere keren “ja”? De volledige Cyberbeveiligingswet (NIS2) starterkit (€79) rekent dit automatisch om naar een indicatie, en geeft u direct de zorgplicht gap-analyse, het informatiebeveiligingsbeleid, de incidentrespons-procedure en een leveranciersvragenlijst-antwoordkit met eerlijke voorbeeldantwoorden. Zie **lerider.com/shop/cyberbeveiligingswet/**.

Dit is GEEN officieel beslisschema en geen wettelijk bindende uitkomst. Gebaseerd op de generieke sector- en omvangsdrempels uit de wet; individuele aanwijzingen en sectorspecifieke uitzonderingen vallen hier mogelijk buiten. Template, geen juridisch advies. Gebaseerd op NCTV-informatie over de Cyberbeveiligingswet (in werking 15 augustus 2026) en de NIS2-richtlijn.