CENTRE FOR CYBERSECURITY BELGIUM

TLP:CLEAR

9 april 2026

REF.: NCCA/JK/INS-001

EX-ANTE TOEZICHT OP ESSENTIËLE ENTITEITEN: Verzoek om informatie met deadline 18 april 2026

Aan alle essentiële NIS2-entiteiten,

Met deze brief **verduidelijkt** de NIS2-inspectiedienst[1] van het Centrum voor Cybersecurity België (CCB)[2] **welke informatie uiterlijk op 18 april 2026 aan het CCB moet worden meegedeeld en verzoekt het alle essentiële NIS2-entiteiten formeel om deze informatie aan het CCB door te geven** via e-mail naar het adres certification@ccb.belgium.be. In geval van gevoelige informatie kan eerst een beveiligde link voor bestandsoverdracht worden aangevraagd.

Sinds de NIS2-wet op 18 oktober 2024 in werking is getreden, moeten alle NIS2-entiteiten met name de nodige cyberbeveiligingsmaatregelen nemen om hun netwerken en informatiesystemen te beschermen. Dit omvat beleid en procedures voor het beoordelen van de doeltreffendheid van maatregelen voor het beheer van cyberbeveiligingsrisico's[3]. Tegelijkertijd is de inspectiedienst bevoegd om toezicht te houden op deze entiteiten[4].

De NIS2-inspectiedienst is bevoegd om toe te zien op de naleving door essentiële en belangrijke entiteiten van maatregelen voor het beheer van cyberbeveiligingsrisico's, met name door toegang te vragen tot alle documenten of informatie die nodig zijn voor de uitoefening van hun toezichtsopdracht en hiervan een kopie te verkrijgen; door het overgaan, ter plaatse of elders, tot elk onderzoek, elke controle en elk verhoor; en door alle informatie in te winnen die zij nodig achten voor de beoordeling van de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's. Bij de uitoefening van deze bevoegdheden om informatie op te vragen, vermeldt de inspectiedienst het doeleinde van het verzoek, de precieze informatie of bewijzen die worden gevraagd en de termijn waarbinnen deze moeten worden verstrekt[5].

De NIS2-inspectiedienst (NCCA) verzoekt alle essentiële entiteiten om de benodigde informatie, zoals hieronder uiteengezet, uiterlijk op 18 april 2026 te verstrekken, zodat de dienst de implementatie van de maatregelen voor het beheer van cyberbeveiligingsrisico's grondig kan controleren.

[1] Zie de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2-wet).
[2] Aangewezen als de nationale cyberbeveiligingsautoriteit krachtens artikel 3, § 1 van het Koninklijk Besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerken en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2-KB).
[3] Art. 30, § 3, 6° NIS2-wet.
[4] Titel 4 van de NIS2-wet.
[5] Zie met name de artikelen 44, § 1 tot en met 2; 48, § 1; en 50, § 1 van de NIS2-wet.

Aan het CCB te verstrekken informatie

Entiteiten die hebben gekozen voor ISO/IEC 27001 (3 mogelijke scenario's)[6]

1) Scenario 1: De organisatie beschikt over een ISO/IEC 27001-certificaat dat is afgegeven door een erkend CAB

Uw organisatie hoeft verder niets te doen. De CAB regelt de administratieve formaliteiten.

2) Scenario 2: De organisatie beschikt over een ISO/IEC 27001-certificaat dat is afgegeven door een niet-erkend CAB

Uw organisatie dient de volgende documenten naar het CCB te sturen[7]:

a. Toepassingsgebied van het certificaat
b. Statement of applicability (SoA) van het certificaat (inclusief alle maatregelen voor cyberbeveiliging die worden of zijn geïmplementeerd, gelijkwaardig aan het CyFun® Basic-niveau)
c. Meest recente (interne) auditrapport waarin de implementatie van deze maatregelen voor cyberbeveiliging wordt beoordeeld

Opmerking: vanaf 18 april 2027 moet de organisatie een certificaat verkrijgen dat is afgegeven door een erkend en geaccrediteerd CAB (de overdracht van bestaande certificeringen kan indien nodig worden uitgevoerd; CAB's beschikken hiervoor over procedures).

3) Scenario 3: De organisatie beschikt nog niet over een ISO/IEC 27001-certificaat

Uw organisatie dient de volgende documenten naar het CCB te sturen[8]:

a. Toepassingsgebied van het toekomstige certificaat
b. Statement of applicability (SoA) van het toekomstige certificaat (inclusief alle maatregelen voor cyberbeveiliging die worden of zijn geïmplementeerd, gelijkwaardig aan het CyFun® Basic-niveau)
c. Het meest recente (interne) auditrapport waarin de uitvoering van deze maatregelen voor cyberbeveiliging wordt beoordeeld

Opmerking: vanaf 18 april 2027 moet de organisatie een certificaat verkrijgen dat is afgegeven door een erkend en geaccrediteerd CAB.

Entiteiten die hebben gekozen voor het CyberFundamentals Framework (CyFun®) (2 mogelijke scenario's)[9]

1) Scenario 1: De organisatie heeft reeds een bewijs van naleving van ten minste het CyFun® zekerheidsniveau Basic verkregen van een erkend CAB

De CAB regelt de administratieve formaliteiten. Uw organisatie hoeft verder niets te doen.

2) Scenario 2: De organisatie heeft nog geen bewijs van naleving van ten minste het CyFun® zekerheidsniveau Basic ontvangen van een erkend CAB

Wij eisen dat er vóór de deadline van 18 april 2026 ten minste een ondertekende overeenkomst met een CAB voor het zekerheidsniveau CyFun® Basic is gesloten, zelfs als de daadwerkelijke verificatie alleen later plaatsvindt. U hoeft geen verdere actie te ondernemen dan genoemde verificatie[10].

[6] Art. 39, lid 1, 1° NIS2-wet en art. 5, § 1, 2° NIS2-KB.
[7] Art. 22, § 1, 2° NIS2-RD, gelezen in samenhang met art. 44, § 1 tot en met 2; 48, § 1; en 50, § 1 NIS2-wet.
[8] Art. 22, § 1, 2° NIS2-KB, gelezen in samenhang met art. 44, § 1 tot 2; 48, § 1; en 50, § 1 NIS2-wet.
[9] Art. 39, lid 1, 1° NIS2-wet en art. 5, § 1, 1° NIS2-koninklijk besluit.
[10] Art. 22, § 1, 1° NIS2-koninklijk besluit

Entiteiten die ervoor hebben gekozen om rechtstreeks door het CCB te worden geïnspecteerd[11]

Uw organisatie moet een formeel verzoek om een inspectie indienen bij het CCB (inspection@ccb.belgium.be).

Inspectie door het CCB is een alternatieve optie die aan essentiële entiteiten wordt aangeboden als onderdeel van de regelmatige conformiteitsbeoordeling, waarbij geen gebruik wordt gemaakt van een CAB. Er dient echter te worden opgemerkt dat deze optie voor de betrokken entiteiten minder voordelig is, aangezien zij **geen vermoeden van conformiteit biedt**. Het betreft dus een louter ad-hoc-controle waarop de entiteit zich niet op dezelfde wijze kan beroepen als op een verificatie of certificering die door een CAB wordt uitgevoerd om zich te verdedigen in geval van een incident. Het **is immers nog steeds aan de entiteit om aan te tonen dat zij aan haar verplichtingen voldoet**[12]. Indien een essentiële entiteit bijvoorbeeld over een certificering beschikt, is het aan het CCB om aan te tonen dat de entiteit niet aan haar verplichtingen voldoet. Het is dan ook een aanzienlijk voordeel om over een dergelijk vermoeden van conformiteit te beschikken.

De conformiteitsbeoordeling die rechtstreeks door het CCB wordt uitgevoerd, **neemt de vorm aan van een inspectieprocedure (met mogelijke administratieve maatregelen en sancties)**[13] **en is niet gratis**[14] – behalve voor entiteiten in de sector overheid waarnaar wordt verwezen in bijlage I van de NIS2-wet, en die niet vallen onder artikel 1 van het Koninklijk Besluit van 4 mei 2016 tot oprichting van de Federale Dienst voor Interne Audit (audit door de FIA als NIS2-CAB).

Met vriendelijke groeten,

Johan Klykens (Signature)

Digitally signed by Johan Klykens (Signature)
Date: 2026.04.09 13:15:46 +02'00'

Johan KLYKENS
Directeur
Nationale Certificatie-instantie voor Cyberbeveiliging (NCCA) – NIS2-inspectiedienst
Centrum voor Cybersecurity België

[11] Art. 39, lid 1, 2° NIS2-wet; art. 5, § 1 en 23, § 1 NIS2-RD.
[12] Art. 42 NIS2-wet.
[13] Art. 48 e.v. NIS2-wet.
[14] Art. 20 NIS2-RD.

Uw antwoordtermijn?

U moet antwoorden binnen de gevraagde termijn[15]. Op uw uitdrukkelijke schriftelijke vraag kunnen we de antwoordtermijn verlengen. U moet dan wel aantonen daarvoor een geldige reden te hebben:

- een grondige reden waaruit blijkt dat er meer tijd nodig is om bewijsmateriaal te verzamelen
- ernstige ziekte of langdurige afwezigheid
- een geval van overmacht

Hoe antwoorden?

U kan ons uw antwoord bezorgen:

- per post: CCB - NCCA – NIS2 Inspectiedienst
  Wetstraat 18, 1000 Brussel
- digitaal: certification@ccb.belgium.be

  Bevat uw antwoord bestanden die te groot of te gevoelig zijn om per e-mail te verzenden? Neem in dat geval contact met ons op, zodat wij u een dienst voor gegevensoverdracht kunnen aanbieden.

U antwoordt niet, te laat of onvolledig?

Omdat de wet u verplicht tot tijdig antwoorden, kunnen we u dan een administratieve maatregel[16] of geldboete[17] opleggen.

Verantwoordingsstukken gevraagd?

U kan ervoor kiezen om de gevraagde verantwoordingsstukken niet mee te sturen met uw antwoord. In dat geval zullen wij op uw adres deze stukken controleren. Dit heeft geen administratieve maatregel of geldboete tot gevolg. U moet ons wel binnen de opgegeven termijn contacteren om een afspraak vast te leggen.

Heeft u vragen?

U kan ons steeds contacteren voor meer informatie. De wetgeving waarnaar we in deze brief verwijzen, kan u raadplegen op https://www.ejustice.just.fgov.be/.

Bescherming van uw persoonsgegevens?

Voor meer informatie over hoe wij uw persoonsgegevens verwerken in overeenstemming met de privacywetgeving kunt u terecht op de website van het CCB: https://ccb.belgium.be/nl/persoonsgegevens.

[15] Artikel 44, § 2 NIS2-wet.
[16] Artikel 58 NIS2-wet.
[17] Artikel 59 NIS2-wet.