Versie 2.0
02/2025

CENTRE FOR CYBERSECURITY BELGIUM

Veelgestelde vragen (FAQ)
NIS2 in België

Het doel van dit document is een antwoord te geven op veelgestelde vragen over het wettelijke NIS2-kader in België. Het is een aanvulling op de informatie die al beschikbaar is op de CCB-website en op Safeonweb@Work.

Versie 2.0 bevat de volgende wijzigingen (nieuwe nummering door invoegingen):

Vragen toegevoegd	Uitgebreide vragen
1.2, 1.6, 1.8, 1.13, 1.15, 1.15.1, 1.15.2, 1.15.3, 1.15.4, 1.15.5, 1.16, 1.16.1, 1.16.2, 1.16.3, 1.16.4, 1.16.5, 1.16.6, 1.16.7, 1.20, 1.21.2, 1.21.3, 1.22, 1.22.1, 1.22.2, 1.22.3, 1.22.4, 1.22.5, 1.22.6, 1.22.7, 1.22.8, 1.22.9, 1.22.10, 1.22.11, 1.22.12 2.2, 2.3, 2.6, 2.7, 2.8, 2.9 3.3.2, 3.4, 3.7, 3.8, 3.9, 3.10, 3.11, 3.13.2, 3.13.3, 3.13.4, 3.13.5, 3.13.6, 3.13.7, 3.13.8, 3.13.9, 3.13.10 4.3, 4.5, 4.7, 4.10, 4.12, 4.16 5.2, 5.3	1.3, 1.5, 1.12, 1.14, 1.17, 1.19, 1.21.1 2.4, 2.5 3.2, 3.3, 3.3.1, 3.6, 3.14 4.2.1, 4.4, 4.6, 4.9, 4.11, 4.14 5.1

Een concordantietabel is beschikbaar aan het einde van het document.

Inhoudsopgave

Afkortingen & Referenties

In dit document worden de volgende afkortingen en verwijzingen gebruikt:

- Aanbeveling (2003/361/EG): Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (beschikbaar op Eur-Lex)
- AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (beschikbaar op Eur-Lex)
- BELAC: Belgische Accreditatie-instelling
- CAB: Conformiteitsbeoordelingsinstantie (*Conformity Assessment Body)*
- CCB: Centrum voor Cybersecurity België (nationale cyberbeveiligingsautoriteit & nationaal CSIRT)
- CSIRT: Computer Security Incident Response Team (in België is het CCB het nationale CSIRT)
- CyFun®: *Cyberfundamentals Framework*, beschikbaar op Safeonweb@Work
- DORA: Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende de digitale operationele weerbaarheid van de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (beschikbaar op Eur-Lex).
- Koninklijk besluit NIS2: Koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)
- NCCN: Nationaal crisiscentrum
- NIS1-richtlijn: Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (beschikbaar op Eur-Lex)
- NIS1-wet: Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)
- NIS2-richtlijn: Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (beschikbaar op Eur-Lex)
- NIS2-wet: Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)

1. Algemeen - Toepassingsgebied

1.1. Wat zijn de doelstellingen van de NIS2-wet?

Richtlijn 2022/2555 ("NIS2") en de Belgische NIS2-wet tot omzetting ervan hebben tot doel de cyberweerbaarheid te versterken door zich te richten op de volgende hoofddoelstellingen:

1) Bescherming op het gebied van cyberbeveiliging voor essentiële diensten die in de Europese Unie worden verleend. In vergelijking met de NIS1-richtlijn, breidt de NIS2-richtlijn het aantal essentiële diensten uit in verschillende zeer kritieke sectoren (bijlage I) of andere kritieke sectoren (bijlage II). Het toepassingsgebied wordt nu voornamelijk bepaald door het gebruik van Europese definities (zoals "type-entiteit") en een omvangscriterium (“size-cap”);
2) Versterking van de maatregelen voor risicobeheer op het gebied van cyberbeveiliging die entiteiten moeten nemen, evenals het melden van significante incidenten (met twee categorieën van entiteiten: essentiële of belangrijke);
3) Aanmoedigen van het delen van informatie over incidenten en risico's op het gebied van cyberbeveiliging tussen de betrokken entiteiten en de nationale CSIRT's;
4) Versterking van het toezicht en de sancties;
5) Zorgen voor Europese en nationale samenwerking.

1.2. Wat is er veranderd tussen de NIS1-wet en de NIS2-wet?

Het toepassingsgebied van NIS2 is aanzienlijk uitgebreid ten opzichte van NIS1, met een belangrijke paradigmaverschuiving. In plaats van te vertrouwen op een formele identificatieprocedure, baseert de NIS2-wet zich nu voornamelijk op twee criteria: de geleverde dienst (type entiteit) in specifieke sectoren of deelsectoren en haar omvang (grote of middelgrote onderneming). Op enkele uitzonderingen na vallen alleen in België gevestigde organisaties onder de NIS2-wet, hetzij als "essentiële" of "belangrijke" entiteiten. Meer informatie over het toepassingsgebied van NIS2 is beschikbaar in sectie 1.3.

De meeste NIS1-entiteiten (operatoren van essentiële diensten of digitale dienstverleners) vallen onder de NIS2-wet en moeten zich registreren als een NIS2-entiteit op het platform van het CCB (https://atwork.safeonweb.be). Entiteiten die zich al hebben geregistreerd voor het systeem voor vroegtijdige waarschuwing (*Early Warning System (*EWS)) van het CCB, moeten zich ook opnieuw registreren. Meer informatie over registratie is beschikbaar in sectie 3.13.1.

De cyberbeveiligingsmaatregelen die NIS2-entiteiten moeten implementeren zijn vergelijkbaar met die onder NIS1, maar de NIS2-wet bevat nu een minimumlijst van specifieke maatregelen. De eisen variëren van het beheer van de toeleveringsketen (*supply chain management*) tot kwetsbaarheidsbeheer (*vulnerability management*) en MFA (*Multi Factor Authentication*) en zijn explicieter en gedetailleerder dan voorheen. Meer informatie over cyberbeveiligingsmaatregelen is beschikbaar in sectie .

De procedure voor het melden van incidenten is nu gedetailleerder en uitgebreider. Wanneer zich een significant incident voordoet, is melding binnen bepaalde termijnen verplicht voor essentiële en belangrijke entiteiten (onverwijld en niet later dan 24 uur voor de vroegtijdige waarschuwing,

72 uur voor de formele incidentmelding en 1 maand voor het eindrapport). Andere incidenten, cyberbedreigingen en bijna-incidenten kunnen ook vrijwillig worden gemeld. Het NIS1-platform voor het melden van incidenten is vervangen door een nieuw onlineformulier, dat voor iedereen toegankelijk is zonder dat een login vereist is (https://notif.safeonweb.be). Meer informatie over het melden van incidenten is beschikbaar in sectie 3.3.

Voor entiteiten die onder de sectoren van het bankwezen en de infrastructuur voor de financiële markt van de bijlagen van de NIS2-wet vallen, is de DORA-verordening (*Digital Operational Resiliance Act,* Verordening betreffende digitale operationele weerbaarheid voor de financiële sector) een *lex specialis*, wat betekent dat deze bepaalde NIS2-verplichtingen vervangt, zoals die met betrekking tot cyberbeveiligingsmaatregelen en rapportageverplichtingen bij incidenten. Meer informatie over DORA is beschikbaar in sectie 1.17.

NIS2 vestigt de nadruk op de aansprakelijkheid van bestuursorganen van NIS2-entiteiten met betrekking tot cyberbeveiliging. Meer informatie over deze aansprakelijkheid is beschikbaar in sectie 3.9.

De uitbreiding van het toepassingsgebied van de sectoren vereist een andere aanpak van het toezicht:

- Essentiële entiteiten worden onderworpen aan een verplichte regelmatige conformiteitsbeoordeling door een conformiteitsbeoordelingsinstantie (CAB) of aan een inspectie door het CCB;
- Belangrijke entiteiten kunnen vrijwillig dezelfde regelmatige conformiteitsbeoordeling ondergaan en zijn in elk geval onderworpen aan controles *ex post*;

Meer informatie over supervisie is beschikbaar in hoofdstuk 4.

Deze nieuwe aanpak van het toezicht bevat ook een uitgebreider regime van administratieve sancties, met verschillende boetes en maatregelen die de toezichthoudende autoriteit ter beschikking heeft. De strafrechtelijke sancties van NIS1 zijn geschrapt. Meer informatie over sancties is beschikbaar in sectie .

Wat de bij het toezicht betrokken autoriteiten betreft, zijn de sectorale overheden van de NIS1 allemaal sectorale overheden van de NIS2 geworden. Wel is hun rol aangepast. Het CCB leidt nu het toezicht voor alle sectoren. Meer informatie over bevoegde autoriteiten is te vinden in sectie 4.1.

1.3. Wat is het toepassingsgebied van de NIS2-wet?

Art. 3 tot 7 NIS2-wet

De NIS2-wet is van toepassing op publieke of private entiteiten die in principe in België zijn gevestigd (er zijn enkele uitzonderingen op deze regel) en die een dienst verlenen binnen de Europese Unie die is opgenomen in bijlage I of II van de wet.

Om als een aan de wet onderworpen entiteit te worden beschouwd, is het voldoende om, ongeacht de rechtsvorm, ten minste één van de in bijlage I of II van de wet genoemde activiteiten binnen de Europese Unie uit te oefenen en ten minste te worden beschouwd als een middelgrote onderneming in de zin van Aanbeveling 2003/361/EG van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (“de size-cap).

Essentiële entiteiten zijn organisaties die een dienst verlenen die is opgenomen in bijlage I en die voldoen aan de definitie van grote onderneming in de zin van Aanbeveling 2003/361/EG.

Belangrijke entiteiten zijn organisaties die een dienst leveren die:

- is opgenomen in bijlage I en voldoet aan de definitie van een "middelgrote onderneming" in de zin van Aanbeveling 2003/361/EG;
- is opgenomen in bijlage II en voldoet aan de definitie van een middelgrote of grote onderneming zoals gedefinieerd in Aanbeveling 2003/361/EG;

Volgens artikel 1 van de bijlage bij Aanbeveling 2003/361/EG is een 'onderneming' iedere eenheid, ongeacht haar rechtsvorm, die een economische activiteit uitoefent. Dit begrip kan overheidsinstanties of publieke entiteiten omvatten wanneer zij kritieke diensten leveren (net als andere private entiteiten) die worden genoemd in de bijlagen van de NIS2-richtlijn.

De 'size-cap'-regel is niet van toepassing op bepaalde types entiteiten zoals overheidsinstanties, geïdentificeerde kritieke entiteiten, verleners van vertrouwensdiensten, registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen.

Het is belangrijk om te benadrukken dat het **toepassingsgebied van de NIS2-wet de hele betrokken entiteit omvat** en niet alleen de activiteiten die in de bijlagen van de wet worden opgesomd.

Tenzij de definitie van het type entiteit (dienst) in de bijlage rekening houdt met het bijkomstige of niet-essentiële karakter van de betrokken activiteit, valt een entiteit binnen het toepassingsgebied van de wet**, zelfs als de betrokken dienst die zij verleent alleen een bijkomstig of niet-essentieel onderdeel is van al haar activiteiten.**

Raadpleeg de volgende secties voor meer informatie.

1.4. Wat is een "entiteit" onder NIS2?

Art. 8, 37° NIS2-wet; Art. 6 (35) NIS2-richtlijn

De NIS2-wet is van toepassing op organisaties die kunnen worden aangemerkt als een "entiteit" in de zin van de wet.

Een "entiteit" wordt in de NIS2-wet als volgt gedefinieerd: "*een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen*".

De NIS2-wet is van toepassing op alle entiteiten afzonderlijk, zelfs als ze gegroepeerd zijn en onder dezelfde holding vallen. Het toepassingsgebied en de verplichtingen van de NIS2-wet moeten dus door elke entiteit afzonderlijk worden geanalyseerd, op basis van de eigen geleverde diensten.

Voor de sector overheid voorziet de NIS2-richtlijn in een specifieke notie van "overheidsinstantie", waardoor de lidstaten rekening kunnen houden met elke entiteit die als zodanig erkend is volgens hun nationale publiek recht.

Het is bijvoorbeeld mogelijk om in de sector overheid verschillende NIS2-entiteiten te onderscheiden binnen één enkele publiekrechtelijke rechtspersoon - op voorwaarde dat er een wettelijk erkend verschil wordt gemaakt tussen de verschillende betrokken overheidsinstanties.

1.5. Hoe de omvang van een entiteit berekenen?

Art. 3, § 1 en 2 NIS2-wet & Aanbeveling 2003/361/EG

Voor het toepassingsgebied van de NIS2-wet wordt de omvang van de entiteit berekend op basis van de regels in de bijlage bij de Aanbeveling 2003/361/EG. De Europese Commissie heeft een gedetailleerde gebruikersgids en een berekeningshulpmiddel ter beschikking gesteld.

Een organisatie komt in aanmerking als middelgrote onderneming als het:

- tussen 50 en 249 mensen in dienst heeft (werknemers, tijdelijk of uitzendpersoneel, eigenaren-managers, partners, etc.) – het personeelsbestand (aantal werkzame personen) berekend in arbeidsjaareenheden (AJE); of
- een jaaromzet van meer dan €10 miljoen tot €50 miljoen, of een jaarlijks balanstotaal van meer dan €10 miljoen tot €43 miljoen heeft.

Voor de toepassing van deze drempels voor financiële gegevens heeft de betrokken organisatie de keuze om ofwel haar jaaromzet ofwel haar totale jaarbalans te gebruiken. **Een van deze twee cijfers kan de drempel voor een grote onderneming overschrijden**, zonder dat dit gevolgen heeft voor de classificatie van een organisatie als middelgrote onderneming.

Een organisatie kwalificeert als een grote onderneming als het:

- 250 of meer werknemers in dienst heeft (werknemers, tijdelijk of uitzendpersoneel, eigenaren-managers, partners, etc.) – personeelsbestand berekend in arbeidsjaareenheden (AJE); of
- een jaarlijkse omzet van meer dan €50 miljoen en een jaarlijks balanstotaal van meer dan €43 miljoen heeft.

Er moet rekening worden gehouden met het feit dat in situaties waarbij "partnerbedrijven" of "verbonden bedrijven" betrokken zijn, een proportionele consolidatie van de gegevens (personeelsbestand en financiële gegevens) van de betrokken entiteit en van deze andere entiteiten moet worden uitgevoerd om de omvang te berekenen.

Behoudens bepaalde uitzonderingen, wordt een onderneming als "partner" beschouwd als ze tussen 25% en 50% van het kapitaal of de stemrechten (afhankelijk van welke van de twee het grootst is) in de betreffende entiteit bezit (of omgekeerd). Dit type relatie beschrijft de situatie van ondernemingen die bepaalde financiële partnerschappen aangaan met andere ondernemingen, zonder dat de eerstgenoemde daadwerkelijk direct of indirect zeggenschap uitoefent over de laatstgenoemde.

Behoudens bepaalde uitzonderingen, wordt een onderneming als "verbonden" beschouwd als ze meer dan 50% van het kapitaal of de stemrechten (afhankelijk van welke het hoogst is) in de betrokken entiteit bezit (of omgekeerd).

In het geval van partnerondernemingen moet de onderneming in kwestie aan haar eigen gegevens een deel van het personeelsbestand en de financiële gegevens van de andere onderneming toevoegen om haar omvang te bepalen. Dit aandeel weerspiegelt het percentage aandelen of stemrechten (het hoogste van de twee). In het geval van verbonden ondernemingen moet de onderneming in kwestie 100% van de gegevens van de verbonden onderneming bij haar eigen gegevens toevoegen.

Als een onderneming bijvoorbeeld een belang van 30% heeft in een andere onderneming, telt zij bij haar eigen cijfers 30% van het personeelsbestand, de omzet en het balanstotaal van de partneronderneming op. Als er meerdere partnerbedrijven zijn, moet dezelfde soort berekening worden gemaakt voor elke partneronderneming dat zich direct stroomopwaarts of stroomafwaarts van de onderneming in kwestie bevindt.

De NIS2-wet voorziet echter in een mechanisme waarmee de nationale cyberbeveiligingsautoriteit (CCB) in geval van een onevenredige situatie rekening kan houden met de mate van onafhankelijkheid van een entiteit ten opzichte van haar partners en verbonden ondernemingen, met name wat betreft de netwerk- en informatiesystemen die zij gebruikt om haar diensten te verlenen en wat betreft de diensten die zij verleent. Deze elementen moeten geval per geval worden aangetoond aan het CCB door de organisatie die er gebruik van wenst te maken. De toepassing van dit mechanisme kan ertoe leiden dat een organisatie wordt geherclassificeerd als een belangrijke entiteit in plaats van een essentiële entiteit of helemaal wordt uitgesloten van het toepassingsgebied van de wet.

Volgens artikel 4 van de bijlage bij de Aanbeveling hebben de in aanmerking te nemen gegevens over het aantal werkzame personen en de financiële gegevens betrekking op de gegevens van het laatste afgesloten boekjaar, berekend op jaarbasis, vanaf de datum van afsluiting van de rekeningen, exclusief btw. Om van de ene groottekwalificatie naar de andere over te gaan, moet de onderneming gedurende ten minste twee opeenvolgende jaren boven of onder een drempel vallen: . Een onderneming die tussen twee drempels schommelt, moet mogelijk meer dan twee jaar teruggaan om haar kwalificatie te bepalen.

Zie ook sectie 1.21.3. en de gedetailleerde handleiding voor het berekenen van de omvang voor meer informatie.

1.6. Waarom lijkt de informatie op de CCB-website en in de FAQ over de size cap te verschillen van de informatie in EU Aanbeveling 2003/361?

De tekst van Aanbeveling 2003/361 verwijst naar 'en' wanneer de drempels van een kmo worden beschreven. De reden hiervoor is dat de Aanbeveling de drempels van de grootste tot de kleinste onderneming beschrijft. Op de website van het CCB en ten behoeve van NIS2 worden deze drempels echter beschreven van de kleinste naar de grootste onderneming, wat resulteert in een andere beschrijving. Zoals hieronder wordt uitgelegd, blijven de drempels hetzelfde:

- "1. Tot de categorie kleine, middelgrote en micro-ondernemingen (kmo's) behoren ondernemingen waar minder dan 250 personen werkzaam zijn en waarvan de jaaromzet (JO) 50 miljoen EUR **niet overschrijdt** en/of het jaarlijkse balanstotaal (JBT) 43 miljoen EUR **niet overschrijdt**."
  - ➔ Tekst zegt kmo = < 250 VTE **en** < 50 mln. JO / < 43 mln. JBT
  - ➔ Dus grote onderneming = > 250 VTE **of** > 50 mln. JO (en/of) > 43 mln. JBT
- "2. Binnen de categorie kmo's is een kleine onderneming een onderneming waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR **niet overschrijdt**."

➔ Tekst zegt kleine onderneming = < 50 VTE **en** < 10 mln. JO/ JBT
➔ Middelgrote onderneming = > 50 VTE **of** > 10 mln. JO (en/of) > 10 mln. JBT, maar niet > 250 VTE **of** > 50 mln. JO (en/of) > 43 mln. JBT

Dit is een logische toepassing van de drempels voor de doeleinden van NIS2.

De official 'SME Wizard' Tool van de Europese Commissie, ontworpen om bedrijven te helpen om na te gaan of ze al dan niet een kmo zijn, bevestigt bovenstaande interpretatie.

Onze NIS2-pagina over Safeonweb@Work vermeldt bijgevolg correct (iets anders geformuleerd in sectie 1.5 hierboven):

> *"De in Aanbeveling 2003/361/EG genoemde drempelwaarden voor middelgrote ondernemingen **overschrijden**, namelijk ten minste 50 arbeidsjaareenheden (AJE) of meer dan € 10 miljoen euro jaaromzet of jaarlijks balanstotaal hebben;"*

Dit wordt ook weergegeven in onze scoping tool.

Iets verderop op de NIS2-pagina staat ook het volgende:

> *"Daarna moet het aantal werkzame personen gecombineerd worden met de financiële bedragen om de definitieve categorisatie te krijgen: een onderneming kan ervoor kiezen om ofwel aan het omzetplafond ofwel aan het balanstotaalplafond te voldoen. **Ze mag een van de financiële maxima overschrijden** zonder gevolgen voor haar kmo-status. We kijken dus **alleen naar het laagste van de twee bedragen**."*

Deze tekst is gebaseerd op de officiële gids van de Europese Commissie over de toepassing van Aanbeveling 2003/361/EG (p. 11).

Er zijn bijgevolg verschillende situaties mogelijk waarbij een entiteit geclassificeerd wordt als een middelgrote onderneming, hetzij op basis van het aantal voltijdse werknemers, hetzij op basis van financiële gegevens, of beide samen. Dit komt overeen met de logica van het woord "of".

Met betrekking tot de kwalificatie van een organisatie als een essentiële of belangrijke entiteit onder de NIS2-wet, is het irrelevant of eerst wordt bepaald of de organisatie een dienst verleent die is opgenomen in de bijlagen bij de wet, of dat eerst de omvang wordt bepaald (of dat de size cap niet van toepassing is). Het eindresultaat zal hetzelfde zijn.

1.7. Welke sectoren en diensten vallen onder de NIS2-wet?

Bijlagen I en II van de NIS2-wet

De betreffende entiteit moet ten minste een van de diensten leveren die zijn opgenomen in bijlage I of II van de wet (zelfs als deze dienst slechts een bijkomstig deel van de activiteiten uitmaakt - behalve wanneer de definitie zelf de hoofd- of bijkomstige aard van de geleverde dienst als criterium gebruikt) uit een van de volgende sectoren:

Zeer kritieke sectoren (bijlage I)	**Andere kritieke sectoren (bijlage II)**
○ Energie (elektriciteit, stadsverwarming en -koeling, aardolie, aardgas, waterstof) ○ Vervoer (lucht, spoor, water, weg) ○ Bankwezen ○ Infrastructuur voor de financiële markt	○ Post- en koeriersdiensten ○ Afvalstoffenbeheer ○ Vervaardiging, productie en distributie van chemische stoffen

○ Gezondheidszorg ○ Drinkwater ○ Afvalwater ○ Digitale infrastructuur ○ Beheer van ICT-diensten ○ Overheid ○ Ruimtevaart	○ Productie, verwerking en distributie van levensmiddelen ○ Vervaardiging (van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek; van informaticaproducten en van elektronische en optische producten; van elektrische apparatuur; van machines, apparaten en werktuigen, n.e.g., van motorvoertuigen, aanhangers en opleggers; van andere transportmiddelen) ○ Digitale aanbieders ○ Onderzoek

Elke dienst die onder de NIS2-wet valt, **wordt gedefinieerd** in bijlage I of II, met een verwijzing naar de definities in de relevante Europese wetteksten of in artikel 8 van de NIS2-wet. Deze definities moeten worden geraadpleegd om de betrokken dienst (type entiteit) te begrijpen. Hiertoe zijn de bijlagen beschikbaar op de website van het Belgisch Staatsblad (na de tekst van de wet).

Zie ook sectie . voor meer informatie over hoe u kunt bepalen welke dienst(en) uw organisatie levert in de Europese Unie en de NIS2 scope test tool.

Zie sectie 1.22 voor meer specifieke informatie over de sectoren.

1.8. Moet de dienst die in de bijlagen wordt genoemd de hoofdactiviteit van de entiteit zijn?

De memorie van toelichting bij de NIS2-wet stelt het volgende over artikel 3 van de wet:

Art. 3 NIS2-wet

> *"Om te worden beschouwd als een publieke of private entiteit van een type dat is opgenomen in bijlage I of II van de wet, is het voldoende om, ongeacht de rechtsvorm, ten minste één van de activiteiten uit te oefenen die zijn opgenomen in bijlage I of II van de wet,* ***zelfs als deze dienst slechts een bijkomstig deel van de activiteiten uitmaakt****, en de in paragraaf 1 bedoelde plafonds te overschrijden of voldoen aan een van de in paragraaf 3 en volgende bedoelde criteria (zie infra)"* (eigen aanduidingen)

Artikel 3 van de NIS2-wet, dat het toepassingsgebied van de wet definieert, verwijst naar de concepten publieke of private entiteiten van een type als bedoeld in bijlage I of II, die een middelgrote of grote onderneming vormen in de zin van de Europese Aanbeveling 2003/361/EG.

Net als de NIS2-richtlijn, betekent dit in de praktijk dat het toepassingsgebied van de NIS2-wet rechtstreeks afhankelijk is van de definities in de bijlagen I en II.

In het algemeen **wordt in de definities geen rekening gehouden met het bijkomstige of niet-essentiële karakter van de activiteit voor de betrokken entiteit** (en heeft dit dus geen invloed op het toepassingsgebied van de NIS2-wet). Er zijn echter enkele beperkte uitzonderingen waarbij het criterium van "voornaamste economische activiteit" of "niet-essentieel onderdeel van de

algemene activiteit" wordt gebruikt in de definities en wel degelijk relevant is (zoals in de sectoren afvalstoffenbeheer, drinkwater of afvalwater).

Alleen in deze beperkte uitzonderingen waarin de definities van de bijlagen **uitdrukkelijk voorzien**, **moet rekening worden** gehouden met het **bijkomstige of niet-essentiële karakter van de activiteit**. Een entiteit kan dus onder het toepassingsgebied van de wet vallen, **ook al is de betreffende dienst die zij verleent alleen een bijkomstig of niet-essentieel onderdeel van al haar activiteiten**, tenzij in de bijlagen anders is bepaald**.**

Er is bijgevolg geen contradictie tussen de memorie van toelichting en de bepalingen van de NIS2-wet (en de bijlagen), en de dienst hoeft alleen de hoofdactiviteit van een entiteit te zijn als deze expliciet in de bijlagen wordt genoemd.

1.9. Kunnen de sectoren die onder de NIS2-wet vallen in de toekomst worden uitgebreid?

Art. 3, § 6 NIS2-wet

De Koning kan sectoren of deelsectoren toevoegen aan de bijlagen I en II na raadpleging van de betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit (CCB) bij een besluit na overleg in de Ministerraad.

Op deze manier kunnen de bijlagen worden uitgebreid als in de toekomst blijkt dat een sector die nog niet onder het toepassingsgebied valt, wel moet worden opgenomen vanwege zijn belang voor kritieke maatschappelijke en/of economische activiteiten.

1.10. Kan een entiteit onder meerdere sectoren vallen?

Art. 8, 34°; 25; 39, lid 2; en 44, §1, lid 2 NIS2-wet.

Het is mogelijk dat dezelfde entiteit binnen verschillende sectoren valt (afhankelijk van al haar activiteiten). In dit geval zijn er een aantal overwegingen om rekening mee te houden:

- Strengere verplichtingen hebben voorrang op minder strenge verplichtingen. Als aan het omvangscriterium wordt voldaan (grote onderneming), zal een entiteit die diensten levert die zowel onder bijlage I als bijlage II vallen, als geheel als essentiële entiteit worden aangemerkt;
- De entiteit kan onder toezicht komen te staan van de nationale cyberbeveiligingsautoriteit (CCB) en verschillende sectorale overheden. Deze autoriteiten zullen met elkaar samenwerken in het kader van het toezicht;
- Een publieke entiteit waarvan de hoofdzakelijke activiteit bestaat uit het verlenen van een dienst die is opgenomen in een andere sector (dan de sector overheid) van de bijlagen bij de wet, valt uitsluitend onder die sector (en niet tegelijkertijd onder die sector en de sector overheid).

1.11. Wat is het verschil tussen "essentiële" en "belangrijke" entiteiten?

Essentiële en belangrijke entiteiten worden voornamelijk onderscheiden in het kader van het toezicht en de sancties. Essentiële entiteiten worden proactief "*ex ante*" en reactief "*ex post*" gecontroleerd. Meer specifiek worden essentiële entiteiten onderworpen aan regelmatige conformiteitsbeoordelingen.

Art. 39-42; 48, §1 en §2; 58 en 59 NIS2-wet.

Belangrijke entiteiten zijn onderworpen aan "*ex post*"-toezicht, d.w.z. op basis van bewijs, aanwijzingen of informatie dat een belangrijke entiteit haar verplichtingen krachtens de wet niet nakomt.

Voor meer informatie over toezicht, zie sectie 4.4.

Voor het overige zijn beide soorten entiteiten onderworpen aan dezelfde verplichtingen, bijvoorbeeld met betrekking tot het melden van incidenten (sectie 3.3.) of het nemen van maatregelen voor het beheer van cyberbeveiligingsrisico's (sectie .).

1.12. Hoe werkt de aanvullende identificatieprocedure?

Op eigen initiatief of -indien van toepassing- op voorstel van de betrokken sectorale overheid, kan de nationale cyberbeveiligingsautoriteit (CCB) binnen een bestaande sector van de bijlagen bij de NIS2-wet, een entiteit als essentieel of belangrijk aanmerken, ongeacht haar omvang, in de volgende gevallen:

Art. 11 NIS2-wet

1. de entiteit is de enige aanbieder, in België, van minstens één dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, met name in een van de sectoren of deelsectoren van de bijlagen I en II van de wet;
2. een verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;
3. een verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;
4. de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in België.

Een ontwerpbeslissing tot identificatie wordt voorgelegd aan de betrokken entiteit en aan de bevoegde sectorale overheden, die binnen zestig dagen een advies kunnen uitbrengen.

Het CCB beoordeelt de identificatie van essentiële en belangrijke entiteiten ten minste om de twee jaar, in overeenstemming met dezelfde procedures en werkt deze indien nodig bij.

1.13. Wat gebeurt er als een NIS2-entiteit wordt verkregen door een andere organisatie?

Als een bedrijf of vereniging een NIS2-entiteit verkrijgt, zal de betrokken NIS2-entiteit nog steeds aan de wet moeten voldoen, zolang de dienst(en) die de organisatie levert en de criteria voor size cap voldaan blijven. De NIS2-kwalificatie van de betrokken entiteit wordt niet overgedragen aan de verkrijgende organisatie of moederorganisatie (als het twee verschillende juridische entiteiten blijven). Natuurlijk kan de verwervende organisatie zelf ook onder de wet vallen als deze binnen de EU zelf een NIS2-dienst verleent en aan de size-cap voldoet.

De kwalificatie als belangrijke entiteit van NIS2 kan veranderen na de verwerving, aangezien de entiteit mogelijk groter wordt volgens de berekeningen van de size cap. Deze kunnen immers na een periode van twee jaar worden herzien (sectie 1.5.). Afhankelijk van de dienst die door de NIS2-entiteit wordt geleverd (bijlagen), kan een grotere omvang leiden tot een nieuwe kwalificatie als essentieel in plaats van belangrijk.

In ieder is het mogelijk dat de verkrijgende organisatie passende maatregelen voor het beheer van cyberbeveiligingsrisico's moet implementeren vanwege de verplichting van de NIS2-entiteit om haar toeleveringsketen te beveiligen of wanneer zij dezelfde netwerk- en informatiesystemen delen (sectie 3.14.).

1.14. Wat betekent "(hoofd)vestiging"? Is de wet alleen van toepassing op Belgische organisaties of ook op andere entiteiten?

Art. 4 NIS2-wet

De Belgische NIS2-wet is in principe van toepassing op **in België gevestigde** entiteiten die hun diensten verlenen of hun activiteiten uitvoeren binnen de EU (vestigingsregime).

Het begrip "entiteit" wordt in artikel 8, 37° van de NIS2-wet gedefinieerd als: *"een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen"*. Zie ook sectie 1.4.

Het vestigingscriterium bestaat uit de daadwerkelijke uitoefening van de activiteit door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm, hetzij via de maatschappelijke zetel, hetzij via een filiaal, hetzij via dochteronderneming, via een bedrijfseenheid, via een fabriek, via een commercieel kantoor, enz.

De NIS2-wet voorziet in drie uitzonderingen op de regel van vestiging in België:

1) aanbieders van openbare elektronische-communicatienetwerken of aanbieders van openbare elektronische-communicatiediensten, wanneer zij deze diensten in België verlenen; (locatie dienst-regime)
2) DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook op aanbieders van onlinemarktplaatsen,

onlinezoekmachines of platformen voor socialenetwerkdiensten, wanneer zij hun hoofdvestiging in België hebben; (hoofdvestigingsregime)
3) wanneer overheidsinstanties door België zijn opgericht.

Om de "hoofdvestiging" van een entiteit te bepalen, moeten de volgende vestigingen in een trapsgewijze volgorde worden bepaald (cascade) (als het eerste criterium niet kan worden bepaald of buiten de EU ligt, wordt het tweede of derde criterium gebruikt):

1° waar de beslissingen met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's hoofdzakelijk worden genomen;
2° waar de entiteit haar cyberbeveiligingsactiviteiten uitvoert;
3° waar de entiteit het grootste aantal werknemers in de Unie heeft.

Indien een entiteit niet in de EU is gevestigd maar een dienst verleent die onderworpen is aan het hoofdvestigingsregime, moet ze een wettelijke vertegenwoordiger aanstellen die gevestigd is in een van de lidstaten waar ze haar diensten verleent. Als deze vertegenwoordiger in België gevestigd is, wordt de entiteit geacht haar hoofdvestiging in België te hebben.

Als een entiteit meerdere vestigingen heeft in verschillende EU-lidstaten en onder het hoofdvestigingsregime valt, zijn de NIS2-verplichtingen volgens het hoofdvestigingsregime alleen van toepassing in de lidstaat waar de hoofdvestiging zich bevindt.

Zie de volgende secties voor complexere scenario's.

1.15. Specifieke vragen met betrekking tot jurisdictie en vestiging (op wie is de wet van toepassing?)

1.15.1. Wat als mijn organisatie diensten verleent die onder het vestigingsregime en het hoofdvestigingsregime vallen? Hoe worden de verschillende jurisdictieregels gecombineerd?

Afhankelijk van het type diensten dat wordt geleverd, kan het zijn dat NIS2-entiteiten verschillende bevoegdheidsregels moeten combineren (een telecom operator kan bijvoorbeeld openbare elektronische-communicatienetwerken aanbieden die vallen onder de plaats dienst-regime, elektriciteit produceren wat valt onder het vestigingsregime en een beheerde beveiligingsdienst die valt onder het hoofdvestigingsregime) en mogelijk onderworpen zijn aan verschillende omzettingswetgevingen en bevoegde autoriteiten (afhankelijk van de betrokken entiteit en de plaats van vestiging).

De verschillende bevoegde nationale autoriteiten zullen samenwerken op het gebied van inspecties en het melden van significante incidenten. Dit betekent echter dat de entiteit, in dit geval, de regels van ten minste twee verschillende lidstaten moet combineren door de strengste regels van één lidstaat toe te passen op al haar diensten. Dit zorgt ervoor dat de regels in meerdere lidstaten correct worden nageleefd.

1.15.2. Wat als een entiteit een dochter/moederbedrijf/filiaal heeft in een andere EU-lidstaat die ook moet voldoen aan NIS2?

Dit hangt af van de dienst die door de betreffende organisatie in de andere lidstaat wordt geleverd. De dochteronderneming/moederonderneming/filiaal moet gekwalificeerd zijn als een "entiteit" onder de NIS2-wet (zie sectie 1.4).

De NIS2-wet **is van toepassing op alle organisaties afzonderlijk**, zelfs als ze gegroepeerd zijn en/of onder dezelfde holding vallen. Het toepassingsgebied en de verplichtingen van de NIS2-wet moeten dus door elke organisatie afzonderlijk worden geanalyseerd, op basis van de eigen geleverde diensten. Het is dus mogelijk dat een dochteronderneming wel aan de NIS2-wetgeving moet voldoen, maar een moederonderneming niet.

De volgende punten geven een meer diepgaande analyse van de verschillende mogelijkheden.

A. De verleende dienst valt niet onder een van de jurisdictie-uitzonderingen (sectie 1.14.)

De organisatie in de andere lidstaat moet zich houden aan de NIS2-wetgeving van de lidstaat waar ze is gevestigd.

Voorbeeld: De moedervennootschap is gevestigd in België en de dochtervennootschap is gevestigd in Frankrijk. Ze verlenen beide diensten in de sector productie, verwerking en distributie van levensmiddelen (bijlage II van de NIS2-wet). Hun geconsolideerd aantal werkzame personen (size cap) is voldoende om als middelgrote onderneming te worden aangemerkt. Het moederbedrijf in België zal NIS2 moeten respecteren in België, en het dochterbedrijf zal NIS2 moeten respecteren in Frankrijk.

B. De geleverde dienst valt onder de uitzondering locatie dienst-regime (elektronische communicatie)

De organisatie in de andere lidstaat moet zich houden aan de NIS2-wetgeving van de lidstaat of lidstaten waar zij haar diensten verleent.

Voorbeeld: De moedermaatschappij is gevestigd in België en de dochtermaatschappij is gevestigd in Luxemburg. De dochteronderneming levert openbare elektronische-communicatienetwerken in België, Luxemburg en Duitsland. Gecombineerd met de gegevens van de moederonderneming is het een grote onderneming. Het moet dus voldoen aan de NIS2-wetten van België, Luxemburg en Duitsland (als essentiële entiteit). In de praktijk zullen de verschillende vereisten moeten worden gecombineerd en zullen de strengste regels moeten worden nageleefd om ervoor te zorgen dat aan alle drie de wettelijke kaders wordt voldaan.

C. De geleverde dienst valt onder het hoofdvestigingsregime

De organisatie in de andere lidstaat moet de NIS2-wet naleven van de lidstaat waar ze haar hoofdvestiging heeft (zie sectie 1.14).

Voorbeeld: Het moederbedrijf is gevestigd in België. Het neemt hoofdzakelijk de beslissingen met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's voor zichzelf en ook voor haar filiaal in Nederland. Het moederbedrijf verleent geen NIS2-dienst en valt dus zelf niet onder NIS2. Het filiaal, gevestigd in Nederland, is een middelgrote onderneming en biedt daar

beheerde diensten aan. Maar omdat de hoofdvestiging in België is, valt het filiaal in België onder NIS2 (en moet het zich bijvoorbeeld alleen in België registreren).

1.15.3. Wat als er binnen dezelfde groep NIS2-entiteiten zijn die in meerdere EU-lidstaten zijn gevestigd?

Wat betreft sectie 1.15.2., afhankelijk van de dienst(en) die door de verschillende organisaties worden aangeboden, kunnen ze onder verschillende jurisdicties binnen de EU vallen.

Het is heel goed mogelijk dat één bedrijf in een groep moet voldoen aan NIS2 in België, terwijl een ander bedrijf bijvoorbeeld moet voldoen aan NIS2 in Polen. Als de groep een holding heeft, zal deze ook moeten analyseren of het onder NIS2 valt vanwege een dienst die het levert (NIS2 is van toepassing op alle organisaties afzonderlijk, maar de omvang wordt berekend op groepsniveau met partners of verbonden ondernemingen).

1.15.4. Een bedrijf dat actief is in een van de NIS2-sectoren moet NIS2 volgen in land A, maar het moederbedrijf in land B niet. Hoe gaat dit in zijn werk?

Het bedrijf nr. 1 moet voldoen aan de verplichtingen in de NIS2-wet van land A. Dit omvat registratie, rapportage van incidenten, cyberbeveiligingsmaatregelen, enz. Het moederbedrijf nr. 2 in land B hoeft niet aan al deze verplichtingen te voldoen omdat het niet onder NIS2 valt.

Er zijn echter nog andere manieren waarop het moederbedrijf beïnvloed kan worden:

1. Als de twee bedrijven dezelfde netwerk- en informatiesystemen delen, vereist de toepassing van NIS2 op bedrijf nr. 1 dat de maatregelen voor het beheer van cyberbeveiligingsrisico's worden genomen op het (de) hele systeem (systemen) en netwerk(en) om alles te beschermen (*all hazards-approach* van de maatregelen voor het beheer van cyberbeveiligingsrisico's van NIS2, zie sectie).
2. De verplichting voor bedrijf nr. 1 in het kader van NIS2 om de beveiliging van zijn toeleveringsketen te garanderen, kan ertoe leiden dat het bedrijf de implementatie van cyberbeveiligingsmaatregelen oplegt aan het moederbedrijf nr. 2 (zie sectie 3.14).

Als de in land A gevestigde entiteit alleen een filiaal (dezelfde juridische entiteit) is van het in land B gevestigde bedrijf, is de gehele juridische entiteit onderworpen aan de NIS2-verplichtingen volgens de NIS2 omzetting in land A (ongeacht waar de netwerk- en informatiesystemen zich fysiek bevinden).

1.15.5. Wat als het (dochter/moeder) organisatie buiten de EU is gevestigd maar diensten verleent in de EU?

In principe vallen organisaties die buiten de EU zijn gevestigd niet onder de NIS2 , tenzij ze in de EU een dienst verlenen die valt onder een van de drie uitzonderingsregels inzake jurisdictie, zoals uitgelegd in sectie 1.14.

Voor de dienst die valt onder het locatie dienst-regime (elektronische communicatie), is de NIS2-wetgeving van toepassing van de lidstaat of lidstaten waar de organisatie die buiten de EU gevestigd is haar diensten verleent.

Als de organisatie die buiten de EU gevestigd is een dienst verleent binnen de EU die binnen het hoofdvestigingsregime valt, moet ze een vertegenwoordiger aanstellen die gevestigd is in een lidstaat waar ze haar diensten verleent. Als deze vertegenwoordiger in België is gevestigd, wordt de entiteit geacht haar hoofdvestiging in België te hebben.

De wet definieert een wettelijke vertegenwoordiger als: *""een in de Europese Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Europese Unie is gevestigd, en die door de nationale cyberbeveiligingsautoriteit kan worden gecontacteerd in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze wet"*.

Om te bepalen of een entiteit diensten aanbiedt binnen de Unie, moet worden nagegaan of de entiteit van plan is diensten aan te bieden aan personen in een of meer lidstaten. De loutere toegankelijkheid in de Unie van de website van de entiteit of een tussenpersoon of van een e-mailadres of andere contactgegevens, of het gebruik van een taal die algemeen wordt gebruikt in het derde land waar de entiteit is gevestigd, moet als onvoldoende worden beschouwd om een dergelijk voornemen vast te stellen. Factoren zoals het gebruik van een taal of een munteenheid die algemeen wordt gebruikt in een of meer lidstaten met de mogelijkheid om diensten in die taal te bestellen, of de vermelding van klanten of gebruikers die zich in de Unie bevinden, kunnen er echter op wijzen dat de entiteit van plan is diensten binnen de Unie aan te bieden.

De vertegenwoordiger moet namens de entiteit optreden en de bevoegde overheden of de CSIRT's moeten zich tot de vertegenwoordiger kunnen richten. De vertegenwoordiger moet expliciet door een schriftelijk mandaat van de entiteit worden aangewezen om namens de entiteit op te treden met betrekking tot de wettelijke verplichtingen van de entiteit, met inbegrip van het melden van incidenten.

Voor meer informatie over het registreren van een organisatie die buiten België is gevestigd, zie sectie 3.13.7.

1.16. Specifieke vragen met betrekking tot groepen organisaties of bedrijven

1.16.1. Hoe het toepassingsgebied van NIS2 beoordelen met betrekking tot een groep organisaties of bedrijven?

Binnen een groep organisaties of bedrijven moet, zoals in de vorige punten is uitgelegd, elke rechtspersoon/organisatie zelf en individueel analyseren of hij al dan niet binnen het toepassingsgebied van NIS2 valt op basis van zijn activiteiten en verleende diensten. Het delen van data, netwerk- of informatiesystemen binnen de groep heeft geen invloed op het toepassingsgebied. Elke organisatie wordt geadviseerd om individueel de uitleg in sectie 1.21 door te nemen.

Opgemerkt moet worden dat binnen een groep organisaties of bedrijven het aantal voltijdsequivalenten en de financiële gegevens geconsolideerd moeten worden op basis van de verschillende regels van Aanbeveling 2003/361. Zie voor meer informatie sectie 1.5.

1.16.2. Welke invloed heeft een NIS2-entiteit op andere organisaties of bedrijven binnen dezelfde groep?

Zie de uitleg van sectie 1.15.4.

1.16.3. Wat als een andere organisatie of bedrijf van dezelfde groep dezelfde netwerk- en/of informatiesystemen gebruikt als een NIS2-entiteit?

Als twee organisaties dezelfde netwerk- en informatiesystemen delen, vereist het vallen van één entiteit in het toepassingsgebied van NIS2 dat de maatregelen voor het beheer van cyberbeveiligingsrisico's worden genomen op alle gedeelde netwerk- en informatiesystemen om alles te beschermen (volgens de "*all hazards approach*" van de maatregelen voor het beheer van cyberbeveiligingsrisico's van NIS2, zie sectie).

1.16.4. Wat als er zowel essentiële entiteiten als belangrijke entiteiten zijn binnen dezelfde groep van organisaties of bedrijven?

De NIS2-wet is van toepassing per juridische entiteit. De entiteiten die niet onder NIS2 vallen, maar wel deel uitmaken van dezelfde groep, zullen niet meer directe gevolgen van NIS2 ondervinden dan wat is beschreven in sectie 1.15.4. Of entiteiten binnen dezelfde groep als essentieel of belangrijk worden aangemerkt, verandert niets aan de situatie.

1.16.5. Wat als een organisatie of bedrijf een contract aangaat met een NIS2-dienstverlener en toestaat dat dit contract/deze dienst door andere organisaties wordt gebruikt?

Een bedrijf X sluit bijvoorbeeld een contract af met een digitale dienstverlener - bedrijf Y (zoals een datacentrumdienst) - en staat vervolgens toe dat dit contract/deze dienst wordt gebruikt door een partnerbedrijf Z. In een dergelijke situatie blijft de NIS2-dienst geleverd door bedrijf Y en niet door bedrijf X (zolang bedrijf X geen rol speelt in de levering van de NIS2-dienst aan bedrijf Z).

1.16.6. Hoe zit het met holdings die (bijna) geen personeel hebben, geen omzet, alleen een positieve balans?

Als een holding geen NIS2-dienst verleent, valt deze niet onder NIS2. Het aantal werknemers en de financiële gegevens van de holding echter wel meegenomen in de size cap-beoordeling van verbonden of partnerondernemingen die een NIS2-dienst verlenen.

Naast deze elementen zijn ook de overwegingen van sectie 1.15.4 van toepassing.

1.16.7. Wat als één organisatie IT-services levert aan andere organisaties binnen dezelfde groep van organisaties of bedrijven?

Binnen een groep van organisaties of bedrijven moet elke afzonderlijke juridische entiteit voor zichzelf en elk afzonderlijk analyseren of zij binnen het toepassingsgebied van NIS2 valt, op basis van haar eigen activiteiten en verleende diensten (het aantal werknemers en de financiële gegevens worden echter in principe geconsolideerd met verbonden of partnerondernemingen (zie sectie 1.5).

Wanneer een rechtspersoon een NIS2-dienst levert (bijv. als aanbieder van beheerde diensten of als aanbieder van cloudcomputingdiensten) aan een andere afzonderlijke rechtspersoon, kan deze onder NIS2 vallen (afhankelijk van de omvang), **zelfs als de activiteit alleen wordt aangeboden aan een beperkt aantal organisaties of bedrijven binnen dezelfde groep.**

De situatie kan echter anders worden bekeken als twee of meer organisaties binnen een groep gegevens, netwerken of systemen met elkaar delen (en samen de relevante kosten delen) en er niet één specifieke organisatie binnen de groep is die enkel beheerde diensten aan de anderen levert.

Zie ook sectie 1.22.6.2 met betrekking tot aanbieders van beheerde diensten.

1.17. Hoe werken de DORA-verordening en de NIS2-richtlijn op elkaar in?

Art. 6 NIS2-wet
Art. 2 & 47 DORA

De NIS2-richtlijn en de bijbehorende omzettingswet zijn gericht op horizontale cyberbeveiligingsmaatregelen in de EU. Het doel is om de algehele cyberbeveiliging in de EU te verbeteren en in het bijzonder om een hoog niveau van cyberbeveiliging te waarborgen voor bepaalde entiteiten die kritiek zijn voor maatschappelijke en economische activiteiten.

De DORA-verordening (Digital Operational Resilience Act) richt zich specifiek op operatoren in de financiële sector. Het doel is om de operationele weerbaarheid van informatiesystemen in de financiële sector te versterken en de bestaande regelgeving op dit gebied te coördineren.

DORA is van toepassing op de in artikel 2 van de verordening genoemde financiële entiteiten. Dit zijn:

- kredietinstellingen;
- betalingsinstellingen;
- aanbieders van rekeninginformatiediensten;
- instellingen voor elektronisch geld;
- beleggingsondernemingen;
- aanbieders van cryptoactivadiensten;
- centrale effectenbewaarinstellingen;
- centrale tegenpartijen;
- handelsplatformen;
- transactieregisters;
- beheerders van alternatieve beleggingsfondsen;
- beheermaatschappijen;

- aanbieders van datarapporteringsdiensten;
- verzekerings- en herverzekeringsondernemingen;
- verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen;
- instellingen voor bedrijfspensioenvoorziening;
- ratingbureaus;
- beheerders van kritieke benchmarks;
- aanbieders van crowdfundingdiensten;
- securitisatieregisters;
- derde aanbieders van ICT-diensten.

Het toepassingsgebied van NIS2 en DORA overlappen elkaar voor bepaalde entiteiten die actief zijn in de sectoren van het bankwezen en de infrastructuur voor de financiële markt. De NIS2-richtlijn voorziet daarom in een *lex specialis-regel*: wanneer er op Europees niveau gelijkwaardige sectorale vereisten bestaan op het gebied van cyberbeveiliging en melding van significante incidenten, hebben deze voorrang op de algemene/sectoroverschrijdende vereisten van NIS2.

Echter derde aanbieders van ICT-diensten die onder DORA vallen, vallen echter niet onder de *lex* specialis-regel en kunnen worden onderworpen aan DORA- en NIS2-verplichtingen.

Het is belangrijk op te merken dat in België gevestigde NIS2-entiteiten in de bancaire en financiële sector zich nog steeds moeten registreren zoals de andere NIS2-entiteiten. Significante incidenten die door DORA-entiteiten worden gemeld via hun eigen meldingsmechanisme, worden door de bevoegde autoriteiten (Nationale Bank van België en FSMA) doorgestuurd naar het CCB.

1.18. Vallen kritieke infrastructuren (of kritieke entiteiten volgens de CER-richtlijn) onder het toepassingsgebied van de NIS2-wet?

Art. 9, 5° en 25, §2 NIS2-wet

De exploitant van een of meer kritieke infrastructuur(en) die is/zijn geïdentificeerd krachtens de wet van 1 juli 2011 inzake de beveiliging en bescherming van kritieke infrastructuur (of als kritieke entiteiten in de zin van Richtlijn 2022/2557 - CER-richtlijn) wordt beschouwd als een essentiële entiteit in de zin van de NIS2-wet.

De NIS2-autoriteiten en de bevoegde autoriteiten onder de wet van 1 juli 2011 (en de CER-richtlijn) werken samen om toezicht te houden op deze entiteiten.

Meer informatie over kritieke infrastructuren is te vinden op de website van het Nationaal Crisiscentrum.

1.19. Kunnen NACE-codes worden gebruikt om te bepalen of een entiteit onder de NIS2-wet valt?

Bijlagen I en II van de NIS2-wet

Sommige van de in de bijlagen I en II opgenomen diensten verwijzen naar NACE-codes. In België gevestigde entiteiten die diensten verlenen die onder deze NACE-codes vallen, moeten daarom zorgvuldig nagaan of de NIS2-wet op hen van toepassing is.

Voor alle entiteiten buiten de gevallen waarin de bijlagen van de NIS2-wet voorzien, zijn NACE-codes **geen voldoende basis** om te bepalen of een entiteit onder de NIS2-wet valt. Sommige NACE-codes kunnen op indicatief door entiteiten worden gebruikt, maar om te bepalen of ze binnen het -vaak restrictievere- toepassingsgebied van de NIS2-wet vallen, is verdere analyse van de precieze dienstverlening vereist. De vermelding van een bepaalde NACE-code op de Kruispuntbank van Ondernemingen (KBO) heeft geen invloed op het toepassingsgebied voor deze types entiteiten.

1.20. Vallen conformiteitsbeoordelingsinstanties onder het toepassingsgebied van de wet?

De diensten die gewoonlijk worden verleend door conformiteitsbeoordelingsinstanties (CAB's) zijn als zodanig niet opgenomen in de lijst van entiteiten van de bijlagen I en II van de NIS2-wet. Dit betekent dat CAB's die hun activiteiten beperken tot de beoordeling van conformiteit niet binnen het toepassingsgebied van de NIS2-wet vallen.

CAB's die aanvullend diensten verlenen die worden beschreven in bijlage I of II van de NIS2-wet, kunnen echter binnen het toepassingsgebied van de wet vallen als ze ook voldoen aan het omvangscriterium, zelfs als deze diensten slechts bijkomstig zijn bij hun hoofdactiviteiten.

1.21. Hoe wordt bepaald of een organisatie binnen het toepassingsgebied van de NIS2-wet valt?

De hieronder beschreven methode beschrijft in detail de verschillende stappen van de redenering met betrekking tot het toepassingsgebied van de NIS2-wet Deze methode beoogt echter niet exhaustief te zijn en is niet de enige methode die kan worden gebruikt.

Deze sectie behandelt de volgende items:

1. Voorafgaand aan het analyseren van de NIS2-wet zelf:
    a. Exploiteert mijn organisatie een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren?
    b. Is mijn organisatie onderworpen aan DORA?
2. Wat is de omvang van mijn organisatie?
3. Welke dienst(en) verleent mijn organisatie in de Europese Unie?
4. Waar in Europa is mijn organisatie gevestigd?
5. Kan mijn organisatie achteraf worden geïdentificeerd of bevindt mijn organisatie zich in de toeleveringsketen van een NIS2-entiteit?

Zie ook onze NIS2 scope test tool.

1.21.1. Voorafgaand aan het analyseren van de NIS2-wet zelf

Voordat we overgaan tot de eigenlijke analyse, moeten we eerst kijken naar twee situaties die een grote invloed hebben op hoe het toepassingsgebied van de NIS2-wet werkt voor de betrokken organisaties.

A. Exploiteert mijn organisatie een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren?

Artikel 3, §4 van de NIS2-wet bepaalt dat de wet automatisch van toepassing is op entiteiten die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren (en in de toekomst op kritieke entiteiten in de zin van de CER-richtlijn), ongeacht hun omvang.

Exploitanten van kritieke infrastructuur hoeven daarom niet te analyseren of hun organisatie binnen het toepassingsgebied van de NIS2 -richtlijn valt: zij worden automatisch aangemerkt als essentiële entiteiten.

B. Is mijn organisatie onderworpen aan DORA?

In België gevestigde entiteiten die onder de DORA-verordening vallen, zijn uitgesloten van de meeste vereisten van de NIS2-wet.

Zie sectie 1.17.

1.21.2. Is mijn organisatie een "entiteit" (groep bedrijven)?

Opdat de wet van toepassing zou zijn, moet een organisatie gekwalificeerd zijn als een "entiteit" volgens artikel 8, 37° van de NIS2-wet: "een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen".

Deze elementen zijn met name belangrijk voor grotere organisaties of groepen bedrijven, waar vestigingen in andere lidstaten, zoals filialen, mogelijk niet onder eigen naam kunnen handelen of rechten kunnen uitoefenen en verplichtingen kunnen hebben. In een dergelijke situatie is de NIS2-wet van toepassing op de vennootschap die de rechtspersoonlijkheid van het filiaal heeft.

1.21.3. Wat is de omvang van mijn organisatie?

Om binnen het toepassingsgebied van de NIS2-wet te vallen, moet een entiteit een bepaalde grootte hebben. Om deze omvang te berekenen, verwijst de NIS2-wet naar Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen. Deze Aanbeveling definieert de drempels waarboven een onderneming (elke entiteit die een economische activiteit uitoefent, ongeacht haar rechtsvorm) kan worden beschouwd als een kleine, middelgrote of grote onderneming. Op enkele uitzonderingen na vallen alleen middelgrote en grote ondernemingen binnen het toepassingsgebied van de NIS2-wet.

Om de omvang te bepalen, moet aan twee voorwaarden worden voldaan: het personeelsbestand (gemeten in jaarlijkse arbeidseenheden (AJE's)[1]) en de financiële bedragen (jaarlijkse omzet en/of jaarlijks balanstotaal).

[1] Arbeidsjaareenheden (AJE's) komen overeen met het aantal personen dat gedurende het gehele referentiejaar in kwestie voltijds in de onderneming of voor rekening van de onderneming heeft gewerkt. Het werk van personen die niet het hele jaar hebben gewerkt, het werk van degenen die in deeltijd hebben gewerkt, ongeacht de duur, en het werk van seizoenarbeiders worden als delen van AJE's geteld.

Het aantal werkzame personen moet worden gecombineerd met de financiële bedragen om de grootte van de onderneming te bepalen: een onderneming kan ervoor kiezen om ofwel aan het omzetplafond ofwel aan het balanstotaalplafond te voldoen. Zij **kan een van de financiële maxima overschrijden zonder dat dit gevolgen heeft voor haar kmo-status**. In principe **houden** we dus **alleen rekening met het laagste van de twee** bedragen.

Voorbeeld 1: een onderneming met 35 AJE's (klein) heeft een jaaromzet van € 1.000.000 (klein) en een jaarlijks balanstotaal van € 50.000.000 (groot). Voor de financiële bedragen kiest ze ervoor om alleen rekening te houden met het kleinste: haar jaarlijkse omzet. Ze is dus een kleine of micro-onderneming.

Voorbeeld 2: een onderneming met 80 AJE's (middelgroot) heeft een jaarlijkse omzet van 1.000.000€ (klein) en een jaarlijks balanstotaal van 70.000.000€ (groot). Voor de financiële bedragen kiest ze ervoor om alleen rekening te houden met het kleinste bedrag: haar jaarlijkse omzet. Aangezien de omzet klein is, maar het personeelsbestand middelgroot, is het een middelgrote onderneming.

Een visueel overzicht van de mogelijkheden voor de omvang van ondernemingen vindt u op onze website.

Als we de verschillende mogelijke groottes combineren met het criterium van de geleverde dienst, krijgen we het volgende toepassingsgebied:

- Een middelgrote onderneming met een personeelsbestand tussen 50 en 249 AJE's of een jaaromzet / jaarlijks balanstotaal van meer dan 10 miljoen €:
  - ➔ Valt binnen het toepassingsgebied als "belangrijke entiteit" als het een dienst verleent die is opgenomen in bijlage II van de wet.
  - ➔ Valt **in principe** binnen het toepassingsgebied als "belangrijke entiteit" als het een dienst verleent die is opgenomen in bijlage I van de wet.
- Een grote onderneming heeft een personeelsbestand van ten minste 250 AJE's of een jaaromzet van meer dan 50 miljoen € en een jaarlijks balanstotaal van meer dan 43 miljoen €:
  - ➔ Valt binnen het toepassingsgebied als "belangrijke entiteit" als het een essentiële dienst verleent die wordt vermeld in bijlage II van de wet.
  - ➔ Valt **in principe** binnen het toepassingsgebied als "essentiële entiteit" als het een dienst verleent die is opgenomen in bijlage I van de wet.

In het bijzonder bepaalt de Aanbeveling dat in het geval van entiteiten die samen als "partnerondernemingen" of "verbonden ondernemingen" worden gegroepeerd, afhankelijk van de gedefinieerde criteria, de gegevens (aantal voltijdse werknemers & financiële gegevens) van de andere entiteiten die deel uitmaken van de groep entiteiten in aanmerking worden genomen om de omvang te berekenen (zie ook sectie 1.5.).

Voor meer informatie over de toepassing van de Aanbeveling raden we u aan de Gebruikersgids bij de definitie van kmo's van de Europese Commissie te raadplegen. Deze bevat alle criteria en visuele voorbeelden om u te helpen de Aanbeveling toe te passen. De Commissie heeft ook een hulpmiddel ontwikkeld om de grootte van uw organisatie te bepalen.

Er zijn echter een paar **uitzonderingen**. De volgende types entiteiten vallen onder het toepassingsgebied van de NIS2-wet, ongeacht hun omvang:

- gekwalificeerde verleners van vertrouwensdiensten (essentieel);

- niet-gekwalificeerde verleners van vertrouwensdiensten (belangrijk als micro-, kleine, middelgrote ondernemingen en essentieel als grote ondernemingen);
- DNS-dienstverleners (essentieel);
- registers van topleveldomeinnamen (essentieel);
- domeinnaamregistratiediensten (alleen voor registratie);
- aanbieders van openbare elektronischecommunicatienetwerken (essentieel);
- aanbieders van openbare elektronischecommunicatiediensten (essentieel);
- entiteiten die op nationaal niveau als kritieke zijn geïdentificeerd volgens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren (essentieel);
- overheidsinstellingen die afhangen van de Federale Staat (essentieel).

In het volgende gedeelte wordt uitgelegd hoe u de definities van de diensten geleverd door deze types entiteiten kunt analyseren.

1.21.4. Welke dienst(en) verleent mijn organisatie in de Europese Unie?

Als de omvang van een entiteit eenmaal bekend is, is het vervolgens noodzakelijk om een gedetailleerde analyse uit te voeren van alle diensten die de entiteit levert, per sector of deelsector. Het is belangrijk om elke dienst in kaart te brengen, zelfs als het slechts een bijkomstige activiteit van de entiteit is (tenzij de definitie van de dienst rekening houdt met het feit of het de hoofd- of bijkomstige dienst is).

De bijlagen I en II (of definities) van de NIS2-wet geven details over de betreffende diensten ("type entiteit"), vaak met een verwijzing naar de overeenkomstige Europese wetgeving of naar de definities in artikel 8 van de wet.

De verschillende sectoren en deelsectoren zijn de volgende:

Zeer kritieke sectoren (bijlage I)	Andere kritieke sectoren (bijlage II)
1. Energie a. Elektriciteit b. Stadsverwarming en -koeling c. Aardolie d. Aardgas e. Waterstof 2. Vervoer a. Lucht b. Spoor c. Water d. Weg 3. Bankwezen 4. Infrastructuur voor financiële markt 5. Gezondheidszorg 6. Drinkwater 7. Afvalwater 8. Digitale infrastructuur 9. Beheer van ICT-diensten (business-to-business) 10. Overheid 11. Ruimtevaart	1. Post- en koeriersdiensten 2. Afvalstoffenbeheer 3. Vervaardiging, productie en distributie van chemische stoffen 4. Productie, verwerking en distributie van levensmiddelen 5. Vervaardiging a. Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek b. Vervaardiging van informaticaproducten en van elektronische en optische producten c. Vervaardiging van elektrische apparatuur d. Vervaardiging van machines, apparaten en werktuigen, n.e.g. e. Vervaardiging van motorvoertuigen, aanhangers en opleggers f. Vervaardiging van andere transportmiddelen 6. Digitale aanbieders 7. Onderzoek

De diensten die de organisatie levert, moeten gelinkt worden aan de eerder vermelde definities. Aan de voorwaarde met betrekking tot de geleverde dienst is dus voldaan als er overeenstemming is tussen de twee. Het is heel goed mogelijk dat een organisatie meerdere van de opgesomde diensten levert in verschillende sectoren (zie sectie 1.10).

Kortom, de "belangrijke" entiteiten en de "essentiële" entiteiten zijn de volgende (met uitzondering van de types entiteiten die aan het einde van de sectie 1.21.3 hierboven worden genoemd):

	Middelgrote onderneming	Grote onderneming
Bijlage I diensten	Belangrijk	Essentieel
Bijlage II diensten	Belangrijk	Belangrijk

1.21.5. Vestiging

In principe is de Belgische NIS2-wet van toepassing op entiteiten **die in België zijn gevestigd en die hun diensten of activiteiten binnen de EU verrichten**.

Het begrip vestiging impliceert eenvoudigweg de daadwerkelijke uitoefening van een activiteit door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm.

Afhankelijk van het type entiteit zijn er echter bepaalde uitzonderingen op de Belgische vestigingsregel. De regels met betrekking tot het territoriale toepassingsgebied van de Belgische NIS2-wet worden uitgelegd in sectie 1.14.

1.21.6. Aanvullende identificatie en toeleveringsketen

Niettegenstaande de bovenvermelde regels kan het CCB, indien nodig, bepaalde entiteiten identificeren die in België gevestigd zijn en actief zijn in de sectoren opgesomd in de bijlagen bij de NIS2-wet. Deze bijkomende identificatie gebeurt in overleg met de betrokken organisatie - zie sectie 1.12.

Ongeacht het toepassingsgebied van de NIS2-wet, mag niet worden vergeten dat een groot aantal organisaties indirect met deze nieuwe wettelijke vereisten te maken krijgt als ze deel uitmaken van de toeleveringsketen van een of meer NIS2-entiteiten. Deze laatste zijn verplicht om de beveiliging van hun eigen toeleveringsketen te garanderen en kunnen daarom contractuele verplichtingen opleggen aan hun directe leveranciers of dienstverleners. Voor meer uitleg, zie sectie 3.14.

1.22. Specifieke vragen met betrekking tot bepaalde types entiteiten en sectoren

1.22.1. Bijlage I - 1. Energie - a) Elektriciteit

1.22.1.1. Vallen organisaties die voornamelijk elektriciteit produceren voor eigen gebruik (inclusief zonnepanelen, enz.) onder het toepassingsgebied van de wet?

Bijlage I NIS2-wet & Richtlijn (EU) 2019/944

Op grond van artikel 3, gelezen in samenhang met bijlage I, punt 1, a), streepje 4, van de NIS2-wet, vallen "producenten zoals gedefinieerd in artikel 2, punt 38 van Richtlijn (EU) 2019/944" onder het toepassingsgebied wanneer zij tenminste als middelgrote ondernemingen worden beschouwd in de zin van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, of de plafonds voor middelgrote ondernemingen overschrijden.

Artikel 2, punt (38), van Richtlijn (EU) 2019/944 definieert **"producent"** als een "natuurlijke persoon of rechtspersoon die elektriciteit opwekt", terwijl **"productie"** wordt gedefinieerd als "de productie van elektriciteit" volgens artikel 2, punt (37), van Richtlijn (EU) 2019/944.

Volgens deze definities kwalificeren entiteiten die zonnepanelen of windturbines exploiteren die zijn aangesloten op het elektriciteitsnet, zelfs als zij de zelf opgewekte elektriciteit hoofdzakelijk zelf verbruiken, als producenten overeenkomstig artikel 2, punt 38, van Richtlijn (EU) 2019/944, en vallen zij bijgevolg onder het toepassingsgebied van NIS2 als zij ten minste een middelgrote onderneming zijn.

Op EU-niveau is echter overeengekomen dat deze "producenten" niet de beoogde zeer kritische entiteiten zijn in de deelsector elektriciteit van de NIS2-richtlijn. Daarom kan op hen een minder streng toezicht worden toegepast.

In België behouden entiteiten die onder de definitie van een dienst in de deelsector elektriciteit vallen**, enkel** omdat ze hoofdzakelijk elektriciteit produceren voor **eigen verbruik**, hun NIS2-kwalificatie (essentieel of belangrijk), maar zijn ze onderworpen aan een minder streng toezicht. In de praktijk moeten zij zich nog steeds registreren, significante incidenten melden en cyberbeveiligingsmaatregelen toepassen, maar het gebruik van een **lager zekerheidsniveau van**

het CyberFundamentals (CyFun®) Framework (bv. Basic) om aan hun verplichtingen te voldoen, wordt als proportioneel beschouwd. Deze oplossing houdt rekening met de vrij beperkte maatschappelijke en economische impact van hun elektriciteitsproductie.

1.22.1.2. Wat valt er onder "exploitanten van laadpunten"?

Bijlage I, deelsector elektriciteit van de NIS2-wet vermeldt "exploitanten van een laadpunt die verantwoordelijk zijn voor het beheer en de exploitatie van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten". Bij gebrek aan bijgevoegde definities moeten de woorden in hun gebruikelijke betekenis worden begrepen.

De definitie houdt de volgende voorwaarden in:

1) Een exploitant van een laadpunt
2) Verantwoordelijk voor het beheer en de exploitatie van dit laadpunt
3) Een laaddienst wordt geleverd aan eindgebruikers (onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten)

Als een supermarkt bijvoorbeeld laadpunten op zijn parking plaatst, kan de supermarket onder NIS2 vallen als hij verantwoordelijk is voor het beheer en de exploitatie van het laadpunt. Dit beheer en deze exploitatie worden vaak contractueel gedelegeerd aan een derde partij, zelfs als de laadpunten gelabeld zijn met de naam van de supermarkt. Een organisatie moet dus concreet nagaan of ze zelf een laadpunt beheert en exploiteert, of dat deze dienst aan een derde organisatie wordt overgelaten.

1.22.2. Bijlage I - 1. Energie - c) Olie

1.22.2.1. Wat valt er onder "exploitanten van oliepijpleidingen"?

De NIS2-wet en de bijlage daarbij geven geen definitie van "exploitanten van oliepijpleidingen". De woorden moeten dus in de gebruikelijke betekenis worden opgevat.

1.22.3. Bijlage I - 2. Vervoer

De sector vervoer omvat verschillende deelsectoren en types entiteiten:

a) Lucht:
    a. Luchtvaartmaatschappijen
    b. Luchthavenbeheerders
    c. Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten aanbieden
b) Spoor:
    a. Infrastructuurbeheerders
    b. Spoorwegondernemingen
c) Water:
    a. Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht
    b. Beheerders van havens
    c. Exploitanten van verkeersbegeleidingssystemen
d) Weg:

a. Wegenautoriteiten
b. Exploitanten van intelligente vervoerssystemen

1.22.4. Bijlage I - 5. Gezondheidszorg

De sector gezondheidszorg omvat verschillende types entiteiten:

- Zorgaanbieders
- EU-referentielaboratoria
- Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen
- Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen
- Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van volksgezondheid als kritiek worden beschouwd

1.22.4.1. Welke organisaties vallen onder de definitie van een zorgaanbieder (ziekenhuizen, woonzorgcentra, residentiële zorg enz.)?

Zorgaanbieders in bijlage I, 5. Gezondheidszorg, verwijzen naar zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad en worden gedefinieerd als: "Een natuurlijk of rechtspersoon of een andere instantie die op het grondgebied van een lidstaat wettelijk gezondheidszorg verstrekt."

Om te bepalen of een organisatie onder de definitie van zorgaanbieder valt, moet worden geverifieerd of er "gezondheidszorg" wordt verleend door deze entiteiten:

1) Gezondheidszorg wordt in die richtlijn gedefinieerd als "gezondheidsdiensten die door gezondheidswerkers aan patiënten worden verstrekt om de gezondheidstoestand van deze laatsten te beoordelen, te behouden of te herstellen, waaronder begrepen het voorschrijven en het verstrekken van geneesmiddelen en medische hulpmiddelen ". Dit kan bijvoorbeeld ook het gebruik van infusen, injecties, enz. zijn
2) De richtlijn definieert "gezondheidswerker" ook als " een arts, verantwoordelijk algemeen ziekenverpleger (verpleegkundige), beoefenaar der tandheelkunde (tandarts), verloskundige of apotheker in de zin van Richtlijn 2005/36/EG of een andere beroepsbeoefenaar die werkzaamheden in de gezondheidszorg verricht die behoren tot een gereglementeerd beroep, als gedefinieerd in artikel 3, lid 1, onder a), van Richtlijn 2005/36/EG, of iemand die krachtens de wetgeving van de lidstaat waar de behandeling plaatsvindt als gezondheidswerker wordt aangemerkt ".

Elke betrokken organisatie moet dus voor zichzelf nagaan of de door de entiteit uitgevoerde activiteiten gezondheidsdiensten/gezondheidszorg door een gezondheidswerker vormen of dat deze entiteiten alleen zorg verlenen.

Onder gezondheidszorg/gezondheidsdiensten vallen bijvoorbeeld: ouderenzorg, psychiatrische zorg, ziekenhuizen, revalidatiecentra, rusthuizen, residentiële zorg, thuisverpleegkundige activiteiten, centra voor ambulante revalidatie, artsen, verpleegkundigen... Entiteiten die zorg verlenen aan mensen met een handicap en gewoon/gespecialiseerd onderwijs kunnen hier ook onder vallen, als er binnen deze entiteiten ook activiteiten in verband met gezondheidszorg worden uitgevoerd.

Entiteiten die in principe geen gezondheidsdiensten verlenen zijn bijvoorbeeld: thuiszorg (er wordt alleen huishoudelijk werk geleverd), kinderopvang...

Het is belangrijk dat elke organisatie haar eigen activiteiten in de praktijk analyseert om na te gaan of ze gezondheidsdiensten levert. Zoals eerder vermeld, moeten alle activiteiten van een entiteit in aanmerking worden genomen om te bepalen of een entiteit een NIS2-entiteit is. Zelfs bijkomstige activiteiten kunnen ertoe leiden dat een entiteit onder NIS2 valt, niet enkel de hoofdactiviteit. Het is ook belangrijk op te merken dat een entiteit die een NIS2-activiteit uitvoert en aan het omvangcriterium voldoet, in zijn geheel onder de NIS2-wet valt (voor al haar netwerk- en informatiesystemen).

1.22.4.2. Wat is het verschil tussen "zorg" en "gezondheidszorg"?

Gezondheidszorg betekent gezondheidsdiensten die door gezondheidswerkers aan patiënten worden verstrekt om de gezondheidstoestand van deze laatsten te beoordelen, te behouden of te herstellen, waaronder begrepen het voorschrijven en het verstrekken van geneesmiddelen en medische hulpmiddelen.

Zorg is een breder begrip en kan bijvoorbeeld ook kinderopvang, thuiszorgactiviteiten, enz. omvatten.

1.22.4.3. Hebben woonzorgcentra en rusthuizen dezelfde verplichtingen als andere zorgaanbieders?

Woonzorgcentra en rusthuizen vallen onder de definitie van een zorgaanbieder (zie sectie 1.22.4.1). Ze zijn daarom, als ze voldoen aan de omvangscriteria en gevestigd zijn in België, ofwel een essentiële ofwel een belangrijke entiteit onder de NIS2-wet.

Op EU-niveau is echter overeengekomen dat deze "zorgaanbieders" niet de beoogde zeer kritische entiteiten in de gezondheidszorgsector van de NIS2-richtlijn zijn. Daarom kan op hen een minder streng toezicht worden toegepast.

In België behouden entiteiten die onder de definitie van zorgaanbieder vallen**, enkel** omdat ze een **rusthuis/woonzorgcentrum** zijn, hun NIS2-kwalificatie (essentieel of belangrijk), maar zijn ze onderworpen aan een minder streng toezicht. In de praktijk moeten ze zich nog steeds registreren, significante incidenten melden en cyberbeveiligingsmaatregelen toepassen, maar het gebruik van een **lager zekerheidsniveau van het CyberFundamentals (CyFun®) Framework** (bv. Basic) om aan hun verplichtingen te voldoen, zal als proportioneel worden beschouwd. Deze oplossing houdt rekening met de vrij beperkte maatschappelijke en economische impact van hun gezondheidsdiensten.

1.22.4.4. Wat als mijn organisatie geen eigen zorgprofessionals in dienst heeft?

Onder NIS2 moet een organisatie zelf een NIS2-dienst verlenen om binnen het toepassingsgebied te vallen. Dit betekent dat organisaties die geen eigen zorgprofessionals in dienst hebben, maar een beroep doen op derden om de gezondheidszorgdienst te verlenen, niet onder het toepassingsgebied zullen vallen als zorgaanbieder.

1.22.4.5. Vallen entiteiten die medische hulpmiddelen vervaardigen onder de NIS2-wet?

Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen) in de zin van artikel 22 van Verordening (EU) 2022/123, vallen binnen bijlage I, sector 5. Gezondheid van de NIS2-wet.

Deze verordening verwijst naar een lijst die moet worden opgesteld door de stuurgroep tekorten aan medische hulpmiddelen (*Executive Steering Group on Shortages and Safety of Medicinal Products*) in geval van een noodsituatie. De lijst verwijst naar categorieën kritieke medische hulpmiddelen die zij in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek beschouwt.

Entiteiten die medische hulpmiddelen vervaardigen, kunnen ook vallen onder bijlage II, sector 5. vervaardiging, deelsector a) Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek. Voor meer informatie over deze deelsector, zie sectie 1.22.11).

Bovendien zullen de meeste entiteiten die medische hulpmiddelen vervaardigen, in de toeleveringsketen van entiteiten uit NIS2 vallen (bv. zorgaanbieders uit bijlage I, sector 5). Entiteiten die onder de NIS2-wet vallen, moeten passende en evenredige maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Een van deze maatregelen is de beveiliging van de toeleveringsketen, inclusief beveiligingsgerelateerde aspecten van de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners. Voor meer informatie over de verplichtingen met betrekking tot de toeleveringsketen (*supply chain)* , zie sectie 3.14.

1.22.4.6. Vallen apotheken onder NIS2?

Apotheken kunnen onder meerdere sectoren van de wet vallen, voornamelijk binnen de sector gezondheidszorg.

Ten eerste, gezien de definitie van een zorgaanbieder, zoals uitgelegd in sectie 1.22.4.1, kunnen apothekers in België in bepaalde situaties injecties en vaccins toedienen. Deze handelingen kunnen worden beschouwd als gezondheidsdiensten, waardoor de apotheken in kwestie binnen het toepassingsgebied van NIS2 vallen. Alles hangt hier dus af van het feit of de apotheker al dan niet gezondheidsdiensten verleent.

Ten tweede zouden apotheken theoretisch "Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen" kunnen uitmaken als ze hun eigen farmaceutische producten onderzoeken en ontwikkelen (zie sectie 1.22.4.7, punt A.). Deze O&O-activiteiten zijn echter in de praktijk meestal voorbehouden aan ondernemingen die gespecialiseerd zijn in farmaceutisch onderzoek.

Ten derde kunnen apotheken ook "Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen bedoeld in sectie C, afdeling 21, van de NACE Rev. 2 vervaardigen" (zie sectie 1.22.4.7, punt B.) zijn, als ze de benodigde NACE-code hebben.

Ten vierde zouden apotheken kunnen vallen onder bijlage II, sector 3. van de vervaardiging, productie of distributie van chemische stoffen via de productie van voorwerpen of de distributie van stoffen of mengsels. Zie voor meer informatie sectie 1.22.9.

Ten slotte kunnen apotheken theoretisch onder bijlage II, sector 5. Vervaardiging vallen als ze medische apparatuur produceren. Zie voor meer informatie sectie 1.22.11.1.

Als apotheek moeten deze vijf verschillende mogelijkheden worden geanalyseerd om te bepalen of ze al dan niet onder NIS2 vallen. Houd er rekening mee dat een apotheek voor deze vijf mogelijkheden ten minste een middelgrote onderneming moet zijn (zie sectie 1.5).

1.22.4.7. Vallen andere gezondheidsgerelateerde bedrijven of bedrijven in de farmaceutische toeleveringsketen onder NIS2?

A. Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen

Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG vallen onder bijlage I, sector gezondheidszorg. Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot:

> *"a) elke enkelvoudige of samengestelde substantie, aangediend als hebbende therapeutische of profylactische eigenschappen met betrekking tot ziekten bij de mens; of*
>
> *b) elke enkelvoudige of samengestelde substantie die bij de mens kan worden gebruikt of aan de mens kan worden toegediend om hetzij fysiologische functies te herstellen, te verbeteren of te wijzigen door een farmacologisch, immunologisch of metabolisch effect te bewerkstelligen, hetzij om een medische diagnose te stellen".*

Het is belangrijk om op te merken dat onderzoeksorganisaties ook binnen bijlage II, sector 7. Onderzoek kunnen vallen. Zie voor meer informatie sectie 1.22.12.

B. Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen

Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen, vallen onder bijlage I, sector gezondheidszorg. Deze entiteiten hebben de volgende NACE-codes:

- 21.10 Vervaardiging van farmaceutische grondstoffen
- 21.20 Vervaardiging van farmaceutische producten

De NACE-code van een Belgische organisatie kan bijvoorbeeld gecontroleerd worden op de website van de Kruispuntbank van Ondernemingen.

C. Entiteiten die chemische stoffen vervaardigen, produceren en distribueren

Deze entiteiten vallen onder de sector vervaardiging, productie en distributie van chemische stoffen uit bijlage II. Meer informatie is te vinden in sectie 1.22.9.

D. Farmaceutische groothandel (verkoop van farmaceutische producten)

De verkoop van farmaceutische producten, aan klanten of aan bedrijven, valt niet expliciet onder de bijlagen van de NIS2-wet. Ze zouden echter onder de distributie van chemische stoffen kunnen vallen als aan de criteria en definities wordt voldaan, zoals uitgelegd in sectie 1.22.9.2.

E. Koeriersdiensten voor medicijnen

Koeriersdiensten voor geneesmiddelen vallen niet onder bijlage I, sector 5. Gezondheidszorg. In bepaalde gevallen kunnen zij echter wel onder bijlage II, sector 1. Post- en koeriersdiensten vallen.

Zie voor meer informatie sectie 1.22.8.

F. Sociale zekerheidsfondsen

Sociale zekerheidsfondsen worden niet expliciet genoemd in de bijlagen van de NIS2-wet. Als deze instellingen privé zijn en alleen deze dienst verlenen, vallen ze niet onder het toepassingsgebied van NIS2.

Openbare sociale zekerheidsfondsen kunnen echter onder de sector Overheid van bijlage I vallen, als ze aan de verschillende voorwaarden voldoet. Zie voor meer informatie sectie 2.1.

G. Leveranciers van software voor de gezondheidszorg

Net als bij aanbieders van andere software, moeten de definities van aanbieders van cloudcomputingdiensten en aanbieders van beheerde diensten worden geanalyseerd. Zie voor meer informatie respectievelijk de secties 1.22.6.1 en 1.22.7. Daarnaast kunnen leveranciers van software voor de gezondheidszorg ook onder de verplichtingen betreffende de toeleveringsketen (*supply chain)* vallen (voor meer informatie, zie sectie 3.14).

H. Gezondheidsdatanetwerken (eHealth)

Aanbieders van gezondheidsdatanetwerken (zoals CoZo, Réseau de Santé Wallon of Réseau de Santé Bruxellois), vallen niet onder de definities van de sector gezondheidszorg in bijlage I.

Dit type entiteiten kan echter ook onder de definities van de sectoren digitale infrastructuur vallen, bijvoorbeeld als aanbieders van datacentrumdiensten, aanbieders van cloudcomputingdiensten of aanbieders van beheerde diensten. Hiervoor moeten ze ten minste een middelgrote onderneming zijn. Dit type entiteiten moet daarom controleren of hun activiteiten overeenkomen met de definities uit deze sector. Voor meer informatie, zie secties 1.22.6 en 1.22.7 hieronder.

Of ze ook onder de sector overheid vallen, hangt af van hun juridische aard. Een van de voorwaarden hierover is dat ze publieke rechtspersonen moeten uitmaken. Zie voor meer informatie sectie 2.1.

1.22.5. Bijlage I - 6. Drinkwater

1.22.5.1. Welke organisaties komen in aanmerking als "leveranciers en distributeurs van voor menselijke consumptie bestemd water"?

De woorden "voor menselijke consumptie bestemd water" zijn gedefinieerd in artikel 2, lid 1 van richtlijn (EU) 2020/2184. Zij hebben betrekking op:

"a) al het water dat onbehandeld of na behandeling bestemd is voor drinken, koken, voedselbereiding of andere huishoudelijke doeleinden, zowel in openbare als in particuliere gebouwen en terreinen, ongeacht de herkomst en of het water wordt geleverd via een distributienet, geleverd uit een tankschip of in flessen of in verpakkingen wordt gedaan, met inbegrip van bronwater;

b) al het water dat in levensmiddelenbedrijven wordt gebruikt voor de vervaardiging, de behandeling, de conservering of het in de handel brengen van voor menselijke consumptie bestemde producten of stoffen;".

De bijlage bij de NIS2-wet voegt hieraan toe dat distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten, zijn uitgesloten. Het woord "essentieel" kan als volgt worden geïnterpreteerd: de distributie van water kan "essentieel" zijn als de distributeur zijn activiteiten niet effectief zou kunnen voortzetten zonder de levering/distributie van water bestemd voor menselijke consumptie.

Voorbeelden van organisaties die onder de definitie vallen zijn dus bedrijven die (gebotteld) water verkopen en die hun activiteiten niet effectief zouden kunnen voortzetten als de verkoop van dit water zou stoppen. Zie ook sectie 1.22.10 over de productie en distributie van levensmiddelen.

1.22.6. Bijlage I - 8. Digitale infrastructuur

1.22.6.1. Wat is precies een aanbieder van cloudcomputingdiensten?

Art. 8 NIS2-wet; Overweging 33 NIS2-richtlijn; NIS2 Impact Assessment

Artikel 8, 29° van de NIS2-wet definieert een aanbieder van cloudcomputingdiensten als " Aanbieder van een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn."

Overweging 33 van de NIS2-richtlijn verduidelijkt dit verder: "*Cloudcomputingdiensten moeten digitale diensten omvatten die beheer op verzoek en brede toegang op afstand ("broad remote access") tot een schaalbare en elastische pool van deelbare computercapaciteit mogelijk maken, ook wanneer deze over verschillende locaties is gedistribueerd. Computercapaciteit omvat middelen zoals netwerken, servers of andere infrastructuur, besturingssystemen, software, opslag, toepassingen en diensten."*

- *De term "brede toegang op afstand" wordt gebruikt om te beschrijven dat de cloudcapaciteiten via het netwerk worden aangeboden en toegankelijk zijn via mechanismen die het gebruik van heterogene thin- of thick-client-platforms bevorderen, waaronder mobiele telefoons, tablets, laptops en werkstations.*
- *De term "schaalbaar" verwijst naar de computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputingdiensten wordt toegewezen teneinde schommelingen in de vraag te kunnen opvangen.*
- *De term "elastische pool" wordt gebruikt ter beschrijving van de computercapaciteit die, afhankelijk van de vraag, ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit snel te kunnen verhogen en verlagen naargelang van het werkvolume.*
- *De term "deelbaar" wordt gebruikt ter beschrijving van de computercapaciteit die ter beschikking wordt gesteld van meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend.*

- *De term "gedistribueerd" wordt gebruikt ter beschrijving van de computercapaciteit die zich op verschillende netwerkcomputers of -apparaten bevindt en waarbij onderlinge communicatie en aansturing plaatsvindt door middel van het doorgeven van berichten.*

De dienstmodellen van cloudcomputing omvatten onder meer infrastructuur als dienst ("Infrastructure as a Service" — IaaS), platform als dienst ("Platform as a Service" — PaaS), software als dienst ("Software as a Service" — SaaS) en netwerk als dienst ("Network as a Service" — NaaS). De invoeringsmodellen van cloudcomputing moeten private, gemeenschaps-, publieke en hybride cloud omvatten. De dienst- en invoeringsmodellen van cloudcomputing hebben dezelfde betekenis als de in de ISO/IEC 17788:2014-norm gedefinieerde benamingen van dienst- en invoeringsmodellen. Het vermogen van de cloudcomputinggebruiker om eenzijdig zelfvoorzienend te zijn, bijvoorbeeld wat servertijd of netwerkopslag betreft, zonder enige menselijke interactie door de cloudcomputingdienstverlener, zou kunnen worden omschreven als beheer op verzoek."

In de 2020 impact assessment van de NIS2 richtlijn[2] gaf de Europese Commissie voorbeelden van ondernemingen die in aanmerking komen als aanbieders van cloudcomputingdiensten. Aanbieders van SaaS, IaaS en PaaS werden expliciet genoemd:

- *SaaS: instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting*
- *IaaS: cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)*
- *PaaS: cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.*

De elementen uit de bovenstaande lijst zijn voorbeelden en dus op geen enkele manier exhaustief of beperkend.

Aanbieders van cloudcomputingdiensten worden dus ruim gedefinieerd en omvatten aanbieders van SaaS, IaaS en PaaS.

1.22.6.2. Wat is een aanbieder van datacentrumdiensten precies?

Een aanbieder van datacentrumdiensten wordt in artikel 8, 30° van de NIS2-wet gedefinieerd als een aanbieder van "een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole".

[2] Commission staff working document. Impact assessment report accompanying the document "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", SWD(2020) 345 final, 16 December 2020, part 2/3, online under https://ec.europa.eu/newsroom/dae/redirection/document/72178, pagina 45.

Overweging 35 van de NIS2-richtlijn stelt bovendien: *"Diensten die worden aangeboden door aanbieders van datacentrumdiensten kunnen niet altijd in de vorm van een cloudcomputingdienst worden verleend. Datacentra maken dan ook niet altijd deel uit van cloudcomputinginfrastructuur. Om alle risico's voor de beveiliging van netwerk- en informatiesystemen te beheren, moet deze richtlijn dan ook van toepassing zijn op aanbieders van datacentrumdiensten die geen cloudcomputingdiensten zijn. [...]*
De term "datacentrumdienst" mag niet gelden voor interne bedrijfsdatacentra die eigendom zijn van en geëxploiteerd worden door de betrokken entiteit, voor eigen doeleinden.".

De uitzondering aan het einde van deze overweging is niet van toepassing wanneer binnen een groep bedrijven een van de bedrijven binnen die groep datacentrumdiensten verleent aan een ander bedrijf.

1.22.7. Bijlage I - 9. Beheer van ICT-diensten (B2B): Wat is precies een aanbieder van beheerde diensten (helpdesk, B2B, enz.)?

Artikel 8, 38° van de NIS2-wet definieert een aanbieder van beheerde diensten als: "Een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de consument ter plaatse of op afstand".

Het is belangrijk op te merken dat twee termen van deze definitie ook gedefinieerd zijn in de NIS2-wet of andere rechtsinstrumenten:

- "ICT-product": een element of groep elementen van een netwerk- of informatiesysteem (Verordening (EU) 2019/881, artikel 2, lid 12);
- "Netwerk- en informatiesystemen" betekent:
    a) een elektronisch communicatienetwerk in de zin van artikel 2, punt 1), van Richtlijn (EU) 2018/1972;
    b) elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, op grond van een programma, een automatische verwerking van digitale gegevens uitvoeren; of
    c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan.

De definitie van een aanbieders van beheerde diensten is relatief uitgebreid en omvat 3 verschillende voorwaarden:

1) de installatie, het beheer, de exploitatie of het onderhoud;
2) Van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen;
3) Via bijstand of actieve administratie (ter plaatse of op afstand).

Deze 3 voorwaarden zijn cumulatief vereist om onder de definitie te vallen. De activiteiten/taken in de definitie sluiten elkaar niet uit. Verschillende ervan kunnen door dezelfde entiteit worden uitgevoerd. Er zijn geen andere voorwaarden om te controleren of een organisatie een aanbieder van beheerde diensten is. De naam 'aanbieder van beheerde diensten' hoeft bijvoorbeeld niet expliciet in een contract te worden gebruikt.

Voorbeelden van aanbieders van beheerde diensten omvatten:

- een helpdesk die operationele ondersteuning biedt aan de gebruikers van een netwerk of toepassing via bijstand op afstand;
- een software developer die op afstand bijstand biedt bij de installatie en/of het onderhoud van zijn toepassingen;
- een onderhoudsdienst voor de netwerken van een klant en andere activiteiten die ter plaatse bij de klant worden uitgevoerd.

Naast de definitie moet de term "business-to-business" in bijlage I van de NIS2-wet worden opgevat als een verwijzing naar alle relaties tussen dienstverleners en andere organisaties/professionals (bedrijven, overheidsinstanties, ambachtslieden, beroepen, verenigingen, entiteiten binnen dezelfde groep enz.) in tegenstelling tot diensten die worden verleend aan het algemene publiek/individuen (“business-to-customers”).Het feit dat een entiteit geen winst maakt of geen commercieel gebruik maakt van de diensten, is geen criterium om een entiteit van deze sector uit te sluiten.

De interpretatie van de begrippen “bijstand” en “actieve administratie” zijn ook belangrijk voor de definitie van een aanbieders van beheerde diensten. Zoals gebruikelijk is bij de juridische interpretatie van Europese teksten, moeten de termen in hun gebruikelijke betekenis worden opgevat als er geen definitie is voorzien in het betreffende rechtsinstrument.

Deze twee begrippen kunnen bijgevolg als volgt geïnterpreteerd worden:

- Voor “bijstand” kan de term betrekking hebben op het verlenen van steun. In de context van een aanbieder van beheerde diensten kan dit inhouden dat klanten worden geholpen wanneer ze problemen ondervinden of wanneer ze richtsnoeren nodig hebben. De term is bijgevolg meer reactief van aard. Er kan ook sprake zijn van probleemoplossing, best practices, hulp bij installatie en configuratie, enz.
- Voor “actieve administratie” lijkt het concept intrinsiek meer proactief. In de context van een aanbieder van beheerde diensten omvat “beheer” in het bijzonder het beheer van en het toezicht op de systemen, toepassingen, netwerken, ... van een klant. Het kan ook systeembewaking, regelmatig onderhoud en updates omvatten, evenals het garanderen van de correcte werking van de betrokken netwerken en informatiesystemen in het algemeen, zonder dat de klant daar per se specifiek om vraagt.

“Op afstand” betekent dat het niet op locatie bij de klant gebeurt (het kan dus vanuit de kantoren van een organisatie zijn).

1.22.8. Bijlage II - 1. Post- en koeriersdiensten: Vallen koeriersdiensten en/of de distributie van medicijnen onder deze sector?

Deze sector omvat aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1 bis van Richtlijn 97/67/EG, met inbegrip van aanbieders van koeriersdiensten. Deze richtlijn bevat meerdere definities:

- Aanbieders van postdiensten: "Een onderneming die een of meerdere diensten levert met betrekking tot postdiensten".
- Postdiensten: "diensten die bestaan in het ophalen, het sorteren, het vervoeren en het bestellen van postzendingen"

Om erachter te komen of dit ook geldt voor koeriersdiensten, moeten we ook kijken naar de wet van 26 januari 2018 met betrekking tot postdiensten (Postwet). Deze bevat de volgende definities:

- Postzending: "geadresseerde zending in de definitieve vorm waarin zij door de aanbieder van postdiensten moet worden vervoerd en waarvan het gewicht niet hoger is dan 31,5 kg".
- Postpakket of pakket: "een postzending die goederen met of zonder handelswaarde bevat, anders dan brievenpost, met een gewicht van ten hoogste 31,5 kg".

Het leveren van een geneesmiddel door een koerier valt binnen het toepassingsgebied van de Postwet (en dus ook onder NIS2-wet) als het voldoet aan de wettelijke criteria, wat vaak het geval blijkt te zijn met betrekking tot de criteria die het begrip pakket definiëren: gewicht minder dan 31.5 kg en een product dat niet is uitgesloten van de postdiensten door artikel 24, § 1, 6° van het koninklijk besluit van 14 maart 2022 betreffende de postdiensten (het is geen narcotisch of psychotroop geneesmiddel, zoals flunitrazepam, het is geen namaakproduct, enz.)

De levering van losse, niet-geïndividualiseerde goederen valt niet onder de definitie van een postpakket en degenen die dergelijke leveringen doen, zijn daarom geen postdienstverleners die onder deze sector van de NIS2-wet vallen.

1.22.9. Bijlage II - 3. Vervaardiging, productie en distributie van chemische stoffen

Deze sector omvat "ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren, als bedoeld in artikel 3, punten 9 en 14, van Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad [(REACH)] en ondernemingen die voorwerpen, zoals gedefinieerd in artikel 3, punt 3, van die verordening produceren uit stoffen of mengsels".

1.22.9.1. Wat wordt bedoeld met "stoffen" en "mengsels

Art. 3, punten (1) & (2) REACH-verordening

Een **stof** wordt gedefinieerd als "*een chemisch element en de verbindingen ervan, zoals zij voorkomen in natuurlijke toestand of bij de vervaardiging ontstaan, met inbegrip van alle additieven die nodig zijn voor het behoud van de stabiliteit ervan en alle onzuiverheden ten gevolge van het toegepaste procedé, doch met uitzondering van elk oplosmiddel dat kan worden afgescheiden zonder dat de stabiliteit van de stof wordt aangetast of de samenstelling ervan wordt gewijzigd*".

Een **mengsel** wordt gedefinieerd als "*een mengsel of oplossing bestaande uit twee of meer stoffen*".

Door te verwijzen naar ondernemingen die zich bezighouden met de vervaardiging van **stoffen** en de distributie van **stoffen** of **mengsels** in de sector "vervaardiging, productie en distributie van chemische stoffen", lijkt de NIS2-wet te verwijzen naar alle chemische stoffen, ongeacht of ze potentieel gevaarlijke industriële chemische stoffen zijn of worden gebruikt in alledaagse producten.

1.22.9.2. Welke types entiteiten vallen onder het toepassingsgebied van NIS2 als ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren?

Onder een fabrikant in de zin van REACH wordt begrepen "*een in de Gemeenschap gevestigde natuurlijke persoon of rechtspersoon die in de Gemeenschap een stof vervaardigt*". Stoffen en mengsels moeten worden begrepen zoals uitgelegd in sectie 1.22.9.1.

Het NIS2 Impact Assessment Report biedt kwalitatieve elementen ter ondersteuning van de opname in het toepassingsgebied van het NIS-kader, waarbij wordt verwezen naar gevaarlijke chemische stoffen. Hoewel dit niet in de wetstekst staat, lijken de verwijzing naar gevaarlijke chemicaliën in het impact assessment rapport te indiceren dat het niet de bedoeling van de wetgever was om bedrijven die chemische elementen van welke soort dan ook vervaardigen of distribueren, op te nemen in het toepassingsgebied.

Er moet ook rekening worden gehouden met de registratieverplichting van de REACH-verordening, aangezien de registratieverplichting een belangrijk instrument is om het doel van de REACH-verordening te waarborgen. Zoals uitgewerkt in de overwegingen (17)-(19) van de REACH-verordening moet alle beschikbare en relevante informatie over stoffen als zodanig, in preparaten of voorwerpen worden bijeengebracht om te helpen bij het in kaart brengen van gevaarlijke eigenschappen, en moeten aanbevelingen betreffende risicobeheersmaatregelen stelselmatig via toeleveringsketens worden doorgegeven, als redelijkerwijs noodzakelijk, om negatieve gevolgen voor de menselijke gezondheid en het milieu te voorkomen. De verantwoordelijkheid voor het beheer van de risico's van stoffen moet liggen bij de natuurlijke of rechtspersonen die deze stoffen vervaardigen, invoeren, in de handel brengen of gebruiken. Om deze reden verplichten de registratiebepalingen de fabrikanten en importeurs ertoe gegevens te verzamelen over de stoffen die zij vervaardigen of invoeren, deze gegevens te gebruiken om de risico's van deze stoffen te beoordelen en geschikte risicobeheersmaatregelen op te stellen en aan te bevelen. Om ervoor te zorgen dat zij deze verplichtingen ook nakomen, en omwille van de transparantie, moeten zij voor de registratie bij het Europees Agentschap voor chemische stoffen een dossier met al deze informatie indienen. Geregistreerde stoffen moeten op de interne markt kunnen circuleren.

Het toepassingsgebied van deze definitie betreft dus in de eerste plaats entiteiten die onder de registratieplicht van de REACH-verordening vallen.

Hoewel andere organisaties die niet registratieplichtig zijn, ook kunnen worden aangemerkt als ondernemingen die **stoffen vervaardigen** en **stoffen of mengsels distribueren** als bedoeld in artikel 3, punten 9 en 14, van REACH, is op EU-niveau overeengekomen dat deze niet de beoogde kritische entiteiten in de chemische sector van de NIS2-richtlijn zijn. Daarom kan op deze entiteiten een minder streng toezicht worden toegepast.

In België blijven entiteiten die onder de definitie van een fabrikant vallen, maar zich niet hoeven te registreren volgens de REACH-verordening, NIS2-entiteiten (essentiële of belangrijke entiteiten), maar zijn ze onderworpen aan een minder streng toezicht. In de praktijk moeten zij zich nog steeds registreren, significante incidenten melden en cyberbeveiligingsmaatregelen toepassen, maar het gebruik van een **lager zekerheidsniveau van het CyberFundamentals (CyFun®) Framework** (bijv. Basic) om aan hun verplichtingen te voldoen, wordt als proportioneel beschouwd. Deze oplossing houdt rekening met de vrij beperkte maatschappelijke en economische impact van hun diensten.

1.22.9.3. Valt een detailhandelaar onder de distributie van stoffen of mengsels?

In bijlage II, punt 3, van de NIS2-wet verwijst de definitie voor de term distributie van chemische stoffen naar artikel 3, punt 14, van Verordening (EG) nr. 1907/2006 (REACH-verordening).

Volgens die verordening is een distributeur "*elke in de Gemeenschap gevestigde natuurlijke persoon of rechtspersoon, met inbegrip van detailhandelaren, die een stof, als zodanig of in een preparaat, uitsluitend bewaart en in de handel brengt ten behoeve van derden*". Punt 12 van artikel 3 van de REACH-verordening definieert het begrip "in de handel brengen" als "*Het aan een derde leveren of beschikbaar stellen, ongeacht of dit tegen betaling dan wel om niet geschiedt. Invoer wordt beschouwd als in de handel brengen*". De definitie omvat het in de handel brengen van een product, ongeacht of dit de eerste keer is dat het product op de markt wordt geïntroduceerd.

Daarom valt een detailhandelaar in chemische stoffen of mengsels binnen deze definitie van distributeur (op voorwaarde dat aan de overige voorwaarden van toepasselijkheid wordt voldaan).

1.22.9.4. Welke types entiteiten vallen onder het toepassingsgebied van NIS2 als ondernemingen die voorwerpen produceren uit stoffen of mengsels?

Ondernemingen die voorwerpen produceren uit stoffen of mengsels, zoals gedefinieerd in artikel 3, punt 3, van Verordening (EG) nr. 1907/2006 (REACH-verordening), vallen onder het toepassingsgebied van de NIS2-wet, wanneer zij als middelgrote onderneming kunnen worden aangemerkt of de plafonds voor middelgrote ondernemingen overschrijden.

Artikel 3, punt 4, van de REACH-verordening definieert de term **"producent van een voorwerp"** als "*elke natuurlijke of rechtspersoon die een voorwerp in de Gemeenschap produceert of assembleert*". Een entiteit is dus een producent van een voorwerp als zij voorwerpen produceert binnen de EU, ongeacht hoe het voorwerp wordt geproduceerd en of het in de handel wordt gebracht.

Voor de definitie van voorwerpen verwijst de NIS2-wet naar artikel 3, punt 3, van de REACH-verordening. Volgens artikel 3, punt 3, van de REACH-verordening wordt onder **"voorwerp"** verstaan "*een object waaraan tijdens de productie een speciale vorm, oppervlak of patroon wordt gegeven waardoor zijn functie in hogere mate wordt bepaald dan door de chemische samenstelling*". Voorbeelden van voorwerpen zijn kleding, vloerbedekking, meubilair, sieraden, kranten en plastic verpakkingen.

Bij de interpretatie van de vraag in hoeverre **producenten van voorwerpen** onder het toepassingsgebied van de NIS2-wet vallen, moet echter rekening worden gehouden met het feit dat de eerste kolom van bijlage II, punt (3), van de NIS2-wet de sector definieert als "vervaardiging, productie en distributie van chemische stoffen" en daarmee een grens stelt aan het toepassingsgebied van de derde kolom van bijlage II, punt (3), voor zover chemische stoffen het voorwerp moeten zijn van de vervaardiging, productie en distributieactiviteit van de entiteiten waarnaar in de derde kolom van bijlage II, punt (3), wordt verwezen.

Bovendien definieert de NIS2-wet in bijlage II, punt (5), een afzonderlijke sector voor vervaardiging, waarbij het toepassingsgebied wordt beperkt tot de vervaardiging van medische hulpmiddelen, medische hulpmiddelen voor in-vitrodiagnostiek, informaticaproducten, elektronische producten, optische producten, elektrische apparatuur, machines, apparaten en

werktuigen, n.e.g. motorvoertuigen, aanhangwagens, opleggers en andere transportmiddelen. Aangezien de definitie van voorwerpen in de REACH-verordening zeer ruim is, zou de specificatie van het toepassingsgebied van de sector vervaardiging in bijlage II, punt 5, zinloos worden indien elke onderneming die voorwerpen produceert zoals gedefinieerd in artikel 3, punt 3, van de REACH-verordening, zou worden beschouwd als vallende onder het toepassingsgebied van bijlage II, punt 3, van de NIS2-wet.

Daarom mogen de types entiteiten waarnaar wordt verwezen in de derde kolom van bijlage II, punt 3, en die in deze sector actief zijn als ondernemingen die uit stoffen of mengsels voorwerpen produceren, zoals gedefinieerd in artikel 3, punt 3, van de REACH-verordening, geen entiteiten omvatten die overeenkomstig bijlage II, punt 5, ook onder het toepassingsgebied van de sector "vervaardiging" vallen.

Het toepassingsgebied van deze definitie heeft dus in de eerste plaats betrekking op entiteiten die onder de REACH-verordening vallen onder de registratie- en meldingsplicht voor stoffen in voorwerpen.

Met betrekking tot andere entiteiten die niet onderworpen zijn aan de registratie- en meldingsplicht voor stoffen in voorwerpen en die ook kunnen worden aangemerkt als ondernemingen die voorwerpen vervaardigen uit stoffen of mengsels, is in het licht van bovenstaande overwegingen op EU-niveau overeengekomen dat deze niet de beoogde kritische entiteiten in de chemische sector van de NIS2-richtlijn zijn. Daarom kan op hen een minder streng toezicht worden toegepast.

In België blijven entiteiten die vallen onder de definitie van een onderneming die voorwerpen vervaardigt uit stoffen of mengsels, maar zich niet hoeven te registreren volgens de REACH-verordening, NIS2-entiteiten (essentiële of belangrijke entiteiten), maar ze zijn onderworpen aan een minder streng toezicht. In de praktijk moeten zij zich nog steeds registreren, significante incidenten melden en cyberbeveiligingsmaatregelen toepassen, maar het gebruik van een **lager zekerheidsniveau van het CyberFundamentals (CyFun®) Framework** (bv. Basic) om aan hun verplichtingen te voldoen, wordt als proportioneel beschouwd. Deze oplossing houdt rekening met de vrij beperkte maatschappelijke en economische impact van hun diensten.

1.22.10. Bijlage II - 4. Productie, verwerking en distributie van levensmiddelen

Deze sector omvat levensmiddelenbedrijven zoals gedefinieerd in artikel 3, punt 2, van Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad, die zich bezighouden met groothandel en industriële productie en verwerking. Een levensmiddelenbedrijf wordt gedefinieerd als "*een onderneming, zowel publiek- als privaatrechtelijk, die al dan niet met winstoogmerk actief is in enig stadium van de productie, verwerking en distributie van levensmiddelen*".

Bijlage II van de NIS2-wet voegt hieraan toe dat deze alleen betrekking heeft op levensmiddelenbedrijven die "zich bezighouden met groothandelsdistributie en industriële productie en verwerking". De nadruk ligt hier op groothandelsdistributie, wat een B2B-factor impliceert (in tegenstelling tot B2C). Deze nadruk is bedoeld om de detailhandel buiten het toepassingsgebied te houden. Op dezelfde manier is "industriële productie en verwerking" bedoeld om productie en verwerking te beperken tot grootschalige productie en verwerking van levensmiddelen.

Het is voldoende dat het levensmiddelenbedrijf een van de volgende activiteiten uitvoert om onder deze sector te vallen: groothandel, industriële productie of industriële verwerking van levensmiddelen. Deze elementen zijn niet cumulatief, maar alternatieve voorwaarden.

Zoals aangegeven in sectie 1.8. is het voldoende dat een van deze drie activiteiten gewoon een bijkomende activiteit van een organisatie is.

1.22.10.1. Vallen supermarkten onder Bijlage II sector 4. Levensmiddelen?

Zoals vermeld in sectie 1.22.10, is de sector productie, verwerking en distributie van levensmiddelen gericht op groothandelsdistributie, industriële productie of industriële verwerking van levensmiddelen. Supermarkten behoren tot de detailhandel. Over het algemeen vallen ze niet onder bijlage II, sector 4.

Als een supermarktketen echter bepaalde levensmiddelen op grote schaal produceert (bijvoorbeeld onder zijn eigenlabel), dan valt de entiteit die deze goederen produceert onder industriële productie en dus onder deze sector. Het feit dat de entiteit deze levensmiddelen produceert met als enig doel haar eigen supermarkten te bevoorraden, maakt geen verschil voor de kwalificatie onder deze sector. De andere entiteiten binnen de supermarktgroep vallen binnen de toeleveringsketen van die entiteit. Voor meer informatie over de toeleveringsketen, zie sectie 3.14.

1.22.10.2. Vallen restaurants onder bijlage II, sector 4 van NIS2?

Zoals vermeld in sectie 1.22.10, is de sector productie, verwerking en distributie van levensmiddelen gericht op groothandeldistributie, industriële productie of industriële verwerking van levensmiddelen. Restaurants vallen in principe niet binnen deze drie mogelijkheden en dus ook niet binnen bijlage II, sector 4 van de NIS2-wet.

Als een restaurantketen echter bepaalde levensmiddelen op grote schaal produceert (bijvoorbeeld onder zijn eigen label), dan valt de entiteit die deze goederen produceert onder industriële productie en dus onder deze sector. Het feit dat de entiteit deze levensmiddelen produceert met als enig doel haar eigen restaurants te bevoorraden, maakt geen verschil voor de kwalificatie onder deze sector. De andere entiteiten binnen de restaurantgroep vallen binnen de toeleveringsketen van die entiteit. Voor meer informatie over de toeleveringsketen, zie sectie 3.14.

1.22.11. Bijlage II - 5. Vervaardiging

1.22.11.1. Wat betekent "vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek"?

Entiteiten die medische hulpmiddelen als gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek als gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen als bedoeld in bijlage I, punt 5, vijfde streepje, van de NIS2-wet vervaardigen, vallen binnen deze deelsector van bijlage II, 5. Vervaardiging.

Een medisch hulpmiddel wordt gedefinieerd als: *" een instrument, toestel of apparaat, software, implantaat, reagens, materiaal of ander artikel dat of die door de fabrikant is bestemd om alleen*

of in combinatie te worden gebruikt bij de mens voor een of meer van de volgende specifieke medische doeleinden:

- *diagnose, preventie, monitoring, voorspelling, prognose, behandeling of verlichting van ziekte,*
- *diagnose, monitoring, behandeling, verlichting of compensatie van een letsel of een beperking,*
- *onderzoek naar of vervanging of wijziging van de anatomie of van een fysiologisch of pathologisch proces of een fysiologische of pathologische toestand,*
- *informatieverstrekking via in vitro-onderzoek van specimens afkomstig van het menselijk lichaam, waaronder orgaan-, bloed- en weefseldonaties,*
- *en waarbij de belangrijkste beoogde werking in of op het menselijk lichaam niet met farmacologische of immunologische middelen of door metabolisme wordt bereikt, maar wel door die middelen kan worden ondersteund.*

De volgende producten worden eveneens aangemerkt als medische hulpmiddelen:

- *hulpmiddelen voor de beheersing of ondersteuning van de bevruchting;*
- *producten die speciaal bestemd zijn voor het reinigen, ontsmetten of steriliseren van hulpmiddelen bedoeld in artikel 1, lid 4, en van die bedoeld in de eerste alinea van dit punt;".*

Een medisch hulpmiddel voor in-vitrodiagnostiek wordt gedefinieerd als: *elk medisch hulpmiddel dat een reagens, een reactief product, een kalibrator, een controlemateriaal, een kit, een instrument, een apparaat, een toestel, software of een systeem is dat afzonderlijk of in combinatie wordt gebruikt, en door de fabrikant is bestemd om te worden gebruikt voor het in-vitro-onderzoek van specimens die afkomstig zijn van het menselijk lichaam, met inbegrip van donorbloed en -weefsel, uitsluitend of hoofdzakelijk met het doel informatie te verschaffen over een of meer van de volgende elementen:*

a) over een fysiologisch of pathologisch proces of een fysiologische of pathologische toestand;
b) over aangeboren lichamelijke of geestelijke beperkingen;
c) over de predispositie voor een medische aandoening of een ziekte;
d) om de veiligheid en de mate van verenigbaarheid met potentiële ontvangers te bepalen;
e) om de respons of de reacties op de behandeling te voorspellen;
f) om therapeutische maatregelen te bepalen of te monitoren.

Recipiënten voor specimens worden ook als medisch hulpmiddel voor in-vitrodiagnostiek beschouwd;".

Daarnaast kunnen entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd, ook onder bijlage I, 5. Gezondheidszorg vallen. Voor meer informatie: sectie 1.22.4.5.

Naast de hierboven beschreven situatie zullen de meeste entiteiten die medische hulpmiddelen vervaardigen, in de toeleveringsketen van NIS2-entiteiten vallen (bijv. zorgaanbieders uit bijlage I, sector 5). Entiteiten die onder de NIS2-wet vallen, moeten passende en evenredige maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Een van deze maatregelen is de beveiliging van de toeleveringsketen, inclusief beveiligingsgerelateerde aspecten van de relaties

tussen elke entiteit en haar directe leveranciers of dienstverleners. Voor meer informatie over de toeleveringsketenverplichting (*supply chain)* (zie 3.14).

1.22.12. Bijlage II - 7. Onderzoek

Onderzoeksorganisaties vallen onder bijlage II, 7. Onderzoek en worden gedefinieerd als " Een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen".

1.22.12.1. Heeft sector 7. onderzoek ook betrekking op sponsors?

Onderzoeksorganisaties vallen onder bijlage II, 7. Onderzoek en worden gedefinieerd zoals hierboven aangegeven.

De NIS2-richtlijn geeft in overweging 36 enige context bij deze definitie:

> *Onderzoeksactiviteiten spelen een sleutelrol bij de ontwikkeling van nieuwe producten en processen. Veel van die activiteiten worden verricht door entiteiten die de resultaten van hun onderzoek delen, verspreiden of exploiteren voor commerciële doeleinden. Die entiteiten kunnen dan ook belangrijke spelers in de waardeketens zijn, zodat de beveiliging van hun netwerk- en informatiesystemen integraal deel uitmaakt van de algemene cyberbeveiliging van de interne markt. Onder onderzoeksorganisaties moeten ook entiteiten worden verstaan die het wezenlijk deel van hun activiteiten richten op toegepast onderzoek of experimentele ontwikkeling in de zin van het "Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development" van de Organisatie voor Economische Samenwerking en Ontwikkeling, om hun resultaten te exploiteren voor commerciële doeleinden, zoals de vervaardiging of ontwikkeling van een product of een proces, de verlening van een dienst, of het in de handel brengen daarvan.*

Volgens het Frascati-handboek (2015) is toegepast onderzoek origineel onderzoek dat wordt uitgevoerd om nieuwe kennis te verkrijgen, en is experimentele ontwikkeling systematisch werk, waarbij gebruik wordt gemaakt van kennis uit onderzoek en praktijkervaring en aanvullende kennis wordt geproduceerd, die gericht is op het produceren van nieuwe producten of processen of op het verbeteren van bestaande producten of processen.

Het commerciële doel wordt breed gedefinieerd en omvat *de vervaardiging of ontwikkeling van een product of een proces, de verlening van een dienst, of het in de handel brengen daarvan*. Als het doel van de onderzoeksactiviteiten de productie van een nieuw product is, dan heeft het onderzoek een commercieel doel.

De diensten van sponsors omvatten geen toegepast onderzoek of experimentele ontwikkelingsactiviteiten, maar alleen de financiering van onderzoeksactiviteiten door een andere organisatie. Deze organisaties, die de eigenlijke NIS2-dienst niet verlenen, vallen dus niet binnen het toepassingsgebied van de NIS2-wet.

1.22.12.2. Zijn onderwijsinstellingen "onderzoeksorganisaties"?

Zoals aangegeven in de definitie in sectie 1.22.12, worden onderwijsinstellingen expliciet uitgesloten. Deze kunnen echter nog steeds onder NIS2 vallen als ze deel uitmaken van de publieke sector. Meer informatie is te vinden in sectie 2.7.

2. Overheidssector

2.1. Hoe is de wet van toepassing op de overheidssector?

Art. 8, 34° en bijlage I, sector 10 (Overheid) NIS2-wet

Art. 8, 34° van de wet definieert een "overheidsinstantie" als een administratieve overheid bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

a) zij is niet van industriële of commerciële aard;
b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een andere sector of deelsector van een van de bijlagen;
c) zij is geen privaatrechtelijke rechtspersoon.

Voor de definitie van het begrip “overheidsinstantie” bepaalt artikel 6, 35) van de NIS2-Richtlijn dat het begrip als zodanig moet worden erkend in overeenstemming met het nationale recht, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom is besloten om te verwijzen naar bestaande begrippen in het Belgische recht die de betrokken entiteiten dekken, zodat de toepassing van verschillende concepten niet wordt vermenigvuldigd.

In dit geval is de definitie gebaseerd op het begrip administratieve overheid bedoeld in artikel 14, §1 , eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State (zie sectie 2.2), waaraan criteria zijn toegevoegd: zij mag niet van industriële of commerciële aard zijn, niet hoofdzakelijk een activiteit uitoefenen die tot een van de andere sectoren of deelsectoren opgenomen in de bijlagen bij de wet en geen privaatrechtelijke rechtspersoon zijn.

Deze definitie moet worden gecombineerd met de categorieën entiteittypen die zijn opgenomen in bijlage I, sector 10 (Overheid):

- Overheidsinstanties die van de Federale Staat afhangen;
- Overheidsinstanties die van de deelgebieden afhangen, geïdentificeerd overeenkomstig artikel 11, § 2, van de wet;
- De hulpverleningszones in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp opgericht door de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

Het begrip afhangen volgt uit artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens die het met name mogelijk maakt om entiteiten te omvatten die deel uitmaken van het federale en gefedereerde niveau, die door deze overheden zijn opgericht, waarvan de activiteiten in hoofdzaak door de overheden worden gefinancierd, waarvan het beheer onderworpen is aan het toezicht door deze overheden of instellingen, hetzij waarvan de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen.

Zie ook de volgende delen van dit hoofdstuk voor meer details.

2.2. Wat is een "administratieve autoriteit"?

Volgens de rechtspraak van de Raad van State is een publiekrechtelijke rechtspersoon automatisch een administratieve overheid in de zin van artikel 14, § 1 van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, als ze bevoegdheden uitoefent in het kader van de uitvoerende macht.

Om te analyseren of een privaatrechtelijke rechtspersoon kan worden aangemerkt als een administratieve overheid, worden de volgende criteria toegepast:

1) opgericht of erkend door de federale, gefedereerde, provinciale of gemeentelijke overheid;
2) uitoefening van een taak van algemeen belang;
3) geen deel uitmaken van de rechterlijke macht of de wetgevende macht;
4) werking bepaald en gecontroleerd door de overheid ;
5) kunnen beslissingen nemen die bindend zijn voor derden (dwingende beslissingsbevoegdheid).

Met deze vijf criteria moet rekening worden gehouden bij het bepalen of een privaatrechtelijke rechtspersoon een administratieve overheid uitmaakt.

2.3. Hoe zit het met organisaties uit de publieke sector die actief zijn in een andere NIS2-sector (zoals een openbaar ziekenhuis, een intergemeentelijke organisatie of een woonzorgcentrum)?

Zoals de definitie in art. 8, 34° aangeeft (zie sectie 2.1) is een overheidsinstantie die hoofdzakelijk een dienst verleent die is opgenomen in een andere sector of deelsector van een van de bijlagen bij de wet**, onderworpen aan de regels van die sector en niet aan die van de sector overheid.**

Dit omvat bijvoorbeeld:

- een intercommunale die gas en/of elektriciteit levert;
- een intergemeentelijke organisatie die drinkwater levert;
- een intergemeentelijke organisatie voor afvalverwerking;
- een openbaar ziekenhuis;
- een openbaar woonzorgcentrum;
- een publieke ICT-dienstverleningsorganisatie;
- een openbare postdienst;
- een openbare luchthaven;
- enz.

Als deze voorbeelden deel uitmaken van een lokale overheidsinstantie (dezelfde juridische entiteit), dan valt de hele organisatie alleen in die sector(en) binnen het toepassingsgebied van de wet. Lokale overheidsinstanties vallen inderdaad niet onder de sector overheid in bijlage I van de NIS2-wet. Zie sectie 2.4 hieronder voor meer informatie over lokale overheidsinstanties.

Als een overheidsinstantie die afhangt van de federale staat of van de gefedereerde entiteiten ook (niet hoofdzakelijk) een dienst verleent die valt onder een andere NIS2-sector (dezelfde juridische entiteit), valt ze onder beide sectoren en moet ze de strengste verplichtingen van beide toepassen

(en zich dus ook in beide sectoren registreren). Wanneer overheidsinstanties die afhangen van de gefedereerde entiteiten onder meerdere sectoren vallen, dienen ze niet te wachten tot ze zijn geïdentificeerd om de verplichtingen die voortvloeien uit de NIS2-wet toe te passen en zich te registreren.

2.4. Vallen lokale overheidsinstanties binnen het toepassingsgebied van de wet?

Art. 8, 34°; bijlage I, sector 10 (Overheid) NIS2-wet

Lokale overheidsinstellingen (gemeenten, provincies, intercommunales, openbare centra voor maatschappelijk welzijn (ocmw's), gemeentebedrijven enz.) **vallen niet automatisch onder de NIS2-verplichtingen.** Ze worden namelijk niet expliciet genoemd in de bijlagen van de NIS2-wet in de overheidssector.

Hoewel lokale overheidsinstanties zoals hierboven opgesomd voldoen aan de definitie van artikel 8, 34° (zie sectie 2.1), hangen ze niet af van de federale Staat, noch van de gefedereerde entiteiten.

Overeenkomstig het beginsel van lokale autonomie dat is vastgelegd in artikel 162 van de Grondwet, mogen lokale besturen, ondanks de uitoefening van een toezichthoudende controle of hun financiering, niet worden beschouwd overheidsinstanties die van de federale staat of van de deelgebieden in de zin van bijlage I van de NIS2-wet.

Deze lokale entiteiten vallen **echter** onder het toepassingsgebied van de NIS2-wet als ze een dienst verlenen die is opgenomen in bijlage I of II van de wet en als ze ten minste als middelgrote onderneming kunnen worden aangemerkt. Hun kwalificatie als essentiële en belangrijke entiteit onder de wet hangt dan af van de geleverde dienst en hun omvang (zie ook sectie 1.5).

Lokale overheidsinstanties kunnen ook worden aangewezen door middel van artikel 11, § 1 (aanwijzing door de nationale cyberbeveiligingsautoriteit - CCB), op voorwaarde dat de raadplegingsprocedure, voorzien in artikel 11, §3, wordt nageleefd. Het initiatief voor een dergelijke aanwijzing kan worden genomen op verzoek van de nationale cyberbeveiligingsautoriteit, de betrokken entiteit of een deelgebied.

2.5. Zijn de verplichtingen van de wet van toepassing op de overheidsinstanties van de gewesten en de gemeenschappen?

Art. 11, §2-3 en bijlage I, sector 10 (Overheid) NIS2-wet

De gemeenschaps- en gewestelijke overheidsinstanties vallen onder sector overheid van de NIS2. Ze worden expliciet vermeld als "Overheidsinstanties die van de deelgebieden afhangen". Dit omvat met name gefedereerde overheidsinstanties, maar ook verschillende overheidsentiteiten die door het gefedereerde niveau worden opgericht, gefinancierd of anderszins beheerd, op voorwaarde dat ze voldoen aan de definitie van artikel 8, 34° van de NIS2-wet (zie sectie 2.1).

De nationale cyberbeveiligingsautoriteit (CCB) moet echter eerst een **formele identificatieprocedure** uitvoeren. Dit houdt in dat op basis van een risicoanalyse de entiteiten

worden geïdentificeerd die diensten verlenen waarvan de verstoring een aanzienlijke impact kan hebben op kritieke maatschappelijke of economische activiteiten.

Overeenkomstig artikel 11, §2 en §3 van de NIS2-wet gebeurt deze identificatie in overleg met de betrokken overheidsinstanties en de regeringen van de gefedereerde entiteiten. Aan het einde van deze procedure kan de gewestelijke of gemeenschapsoverheidsinstantie worden aangewezen als essentiële entiteit of belangrijke entiteit.

Als een overheidsinstantie die afhangt van een gefedereerde entiteit ook actief is in een andere sector van de NIS2-wet, is het hierboven beschreven identificatieproces niet nodig voor de toepassing van de NIS2-wet (zie ook sectie 2.3).

Zie sectie 2.8 voor informatie over de registratie.

2.6. Welk personeel moet in rekening worden gehouden om de omvang van mijn (lokale) overheidsinstantie te berekenen?

Zolang een gefedereerde overheidsinstantie of een lokale overheidsinstantie niet formeel geïdentificeerd is als een NIS2-entiteit en afhankelijk van de geleverde diensten, kan het zijn dat ze de omvang moet berekenen.

Overheidsinstanties moeten rekening houden met al het personeel dat werkzaam is **binnen de juridische entiteit** van die overheidsinstantie. Volgens de Gebruikersgids voor de definitie van kmo's van de Europese Commissie *"[omvat] het criterium van aantal werkzame personen voltijds, deeltijds, tijdelijk en seizoenspersoneel:*

- *werknemers;*
- *personen die voor de onderneming werken en bij haar gedetacheerd zijn en volgens het nationale recht als werknemers beschouwd worden (dit kunnen ook tijdelijke werknemers of uitzendkrachten zijn*);
- *eigenaren-managers;*
- *partners die een regelmatige activiteit in de onderneming uitoefenen en financiële voordelen uit de onderneming halen."*

Dit omvat niet:

- *"leerlingen of studenten die een beroepsopleiding volgen en een leer- of beroepsopleidingsovereenkomst hebben;*
- *werknemers met zwangerschaps- of ouderschapsverlof."*

Het basisaantal werkzame personen dat nodig is voor de berekening van de size cap (zie sectie 1.5) wordt uitgedrukt in AJE's (Annual Work Units - arbeidsjaareenheden). Iedereen die gedurende het hele referentiejaar voltijds binnen of voor een onderneming heeft gewerkt, telt als één eenheid. Deeltijds personeel, seizoenarbeiders en degenen niet het hele jaar werkten, worden behandeld als fracties van één eenheid.

In dit verband moet iemand die alleen een deel van het jaar op basis van een arbeidsovereenkomst voor bepaalde tijd of een opdracht heeft gewerkt, als een fractie van een eenheid worden geteld op basis van het aantal gewerkte dagen in het voorgaande jaar (gedeeld door het aantal werkdagen in het jaar).

Personeel dat door een openbaar centrum voor maatschappelijk welzijn (ocmw) ter beschikking wordt gesteld om in een organisatie te werken krachtens artikel 60, §7 van de organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn, wordt in de berekening van het personeelsbestand opgenomen als uitzendkracht.

Het is belangrijk op te merken dat de bepalingen over consolidatie van gegevens van partnerondernemingen en verbonden ondernemingen uit Aanbeveling 2003/361/EG niet van toepassing zijn op overheidsdiensten. Dit betekent dat alleen de gegevens van de overheid zelf in aanmerking moeten worden genomen. Als een gemeente die drinkwaterdiensten levert bijvoorbeeld ook een school heeft, moet alleen rekening worden gehouden met de gegevens van de school als die school deel uitmaakt van dezelfde juridische entiteit als de gemeente.

2.7. Vallen openbare onderwijsinstellingen, scholen of universiteiten onder het toepassingsgebied van de wet?

Enerzijds wordt de onderwijssector niet expliciet genoemd in bijlagen I en II van de NIS2-wet. Privaatrechtelijke onderwijsinstellingen vallen dus niet onder het toepassingsgebied van de NIS2-wet.

Bijlagen I en II & art. 8, 34° NIS2-wet

Anderzijds kunnen **publiekrechtelijke** onderwijsinstellingen, zoals openbare universiteiten of openbare middelbare scholen, worden opgenomen in de definitie van een "overheidsinstantie". Daartoe moeten zij

- voldoen aan het omvangscriterium (zie sectie 1.5);
- gevestigd zijn in België (zie sectie 1.14);
- voldoen aan de definitie van overheidsinstantie in artikel 8 van de NIS2-wet (zie secties 2.1 en 2.2);
- afhangen van de federale staat of de gefedereerde entiteiten (zie sectie 2.1).
- indien afhangen van de gefedereerde entiteiten: geïdentificeerd worden in overeenstemming met art. 11, § 2 (zie sectie 2.5).

Bovendien kan een onderwijsinstelling ook worden aangemerkt als een "zorgaanbieder" (zie sectie 1.22.4.1) in de zin van bijlage I van de NIS2-wet als zij bijvoorbeeld een universitair ziekenhuis beheert dat deel uitmaakt van dezelfde rechtspersoon (als dat niet het geval is, valt alleen het ziekenhuis onder het toepassingsgebied als de size cap wordt bereikt).

2.8. Wanneer en hoe moeten publieke entiteiten zich registreren?

Afhankelijk van de betrokken entiteiten uit de publieke sector zijn verschillende regimes van toepassing:

- Voor overheidsinstanties die afhangen van de federale staat, geldt sinds de inwerkingtreding van de wet de normale deadline voor registratie (tot 18e maart 2025).
- Voor overheidsinstanties die afhangen van gefedereerde entiteiten is de deadline voor registratie gelijk aan 5 maanden nadat de betrokken entiteit formeel is geïdentificeerd door het CCB (identificatiebrief).
- Voor hulpverleningszones geldt sinds de inwerkingtreding van de wet de normale deadline voor registratie (tot 18 maart 2025).

Het is belangrijk op te merken dat deze deadlines enkel gelden als de betrokken organisatie alleen tot de sector overheid behoort. Als de organisatie ook tot een andere sector behoort, kunnen er striktere deadlines gelden.

De registratie vindt plaats op ons Safeonweb@Work-platform (zie sectie 3.13.1).

2.9. Gelden er sancties voor overheidsinstanties? Wat als de organisatie ook tot een andere sector behoort?

Volgens artikel 62 van de NIS2-wet kunnen alle in sectie 4.18.1 vermelde administratieve maatregelen worden genomen als reactie op een overtreding van de wet door overheidsinstanties. Deze entiteiten kunnen echter niet worden onderworpen aan de administratieve geldboetes van sectie 4.17 en sommige specifieke administratieve maatregelen.

Deze uitspraken gelden ook als een overheidsinstantie tegelijkertijd tot de sector overheid en tot een andere NIS2 -sector behoort (het gunstigste regime heeft voorrang).

Een overheidsinstantie die hoofdzakelijk een activiteit uitvoert die is opgenomen in de kolom soort entiteit van een andere sector of deelsector, kan echter worden onderworpen aan administratieve geldboetes en specifieke administratieve maatregelen (omdat ze niet onder de definitie van een overheidsinstantie vallen).

3. Verplichtingen

3.1. Wat zijn de wettelijke verplichtingen voor de betrokken entiteiten?

De NIS2-wet legt een aantal verplichtingen op aan essentiële en belangrijke entiteiten:

- het nemen van passende cyberbeveiligingsmaatregelen;
- de tijdige melding van significante incidenten;
- de registratie bij de bevoegde autoriteiten;
- de opleiding van bestuursorganen (sectie 3.11);
- de periodieke conformiteitsbeoordelingen (verplicht voor essentiële entiteiten en vrijwillig voor belangrijke entiteiten);
- informatie-uitwisseling en samenwerking met de relevante autoriteiten.

Deze verschillende verplichtingen worden in de volgende delen uitgelegd.

3.2. Wat zijn de verplichtingen op het gebied van cyberbeveiligingsmaatregelen?

Art. 30, 31 en 42 NIS2-wet

Essentiële en belangrijke entiteiten moeten passende en evenredige (technische, operationele en organisatorische) maatregelen nemen om de risico's te beheersen die een bedreiging vormen voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten gebruiken bij het uitvoeren van hun activiteiten of het verlenen van hun diensten, en om de gevolgen van incidenten voor de ontvangers van hun diensten en op andere diensten weg te nemen of te beperken.

Het is belangrijk om te benadrukken dat, in tegenstelling tot de NIS1-wet, het **toepassingsgebied van de NIS2-wet de hele betrokken entiteit omvat** en niet alleen de activiteiten die zijn opgenomen in de bijlagen bij de wet.

Om de praktische uitvoering van deze cyberbeveiligingsmaatregelen te vergemakkelijken, heeft het CCB al een raamwerk ontwikkeld en gratis ter beschikking gesteld aan de betrokken entiteiten: het Cyberfundamentals Framework "(CyFun®) met verschillende niveaus en een analysetool om het meest geschikte niveau te bepalen. De wet en het uitvoeringsbesluit bieden essentiële en belangrijke entiteiten die besluiten het CyFun®-kader of de internationale norm ISO/IEC 27001 (met het toepassingsgebied in lijn met NIS2 - d.w.z. alle netwerk- en informatiesystemen) te gebruiken, een **vermoeden van conformiteit** met betrekking tot beveiligingsmaatregelen.

De minimummaatregelen in de wet zijn gebaseerd op een ‘alle risico’s omvattende’- aanpak (*all hazards approach*)" die erop gericht is netwerk- en informatiesystemen en hun fysieke omgeving te beschermen tegen incidenten, en omvatten ten minste het volgende:

1. beleid inzake risicoanalyse en beveiliging van informatiesystemen;
2. incidentenbehandeling;
3. bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;

4. de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
5. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
6. beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
7. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
8. beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
9. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
10. wanneer gepast, het gebruik van multifactorauthenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;
11. een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

De door essentiële en belangrijke entiteiten te nemen maatregelen moeten **passend en evenredig** zijn. Op dit punt is het belangrijk te specificeren dat, om onevenredige financiële en administratieve lasten voor essentiële en belangrijke entiteiten te vermijden, de maatregelen voor risicobeheer op het gebied van cyberbeveiliging **evenredig moeten zijn met de risico's waaraan** het netwerk- en informatiesysteem in kwestie zijn blootgesteld. In dit verband moeten entiteiten met name rekening houden met **de stand van de techniek** van deze maatregelen en, indien van toepassing, met relevante Europese of internationale **normen**, en met de **kosten van de tenuitvoerlegging van** deze maatregelen.

Er moet worden opgemerkt dat sommige NIS2-entiteiten de uitvoeringsverordening 2024/2690 van de Commissie van 17 oktober 2024 moeten volgen, waarin de technische en methodologische vereisten van maatregelen voor het beheer van cyberbeveiligingsrisico's in detail worden beschreven (zie sectie 5.1).

3.3. Wat zijn de verplichtingen met betrekking tot het melden van incidenten?

Meer informatie over het melden van incidenten is te vinden op onze website en in onze gids voor het melden van incidenten.

3.3.1. Algemene regels

Art. 8, 5° en 57°; 34 en 35 NIS2-wet

De wet definieert een incident als *"een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt"*.

In het geval van een significant incident, moet de entiteit dit aan het nationale CSIRT (CCB) melden en, in bepaalde gevallen, ook de ontvangers van hun diensten op de hoogte stellen.

Zie onze gids voor het melden van incidenten voor meer informatie over "significante" incidenten.

De melding vindt plaats in verschillende fasen (zie sectie 3.3.4): eerst een vroegtijdige waarschuwing binnen 24 uur nadat het incident is ontdekt (*early warning*), vervolgens een formele incidentmelding binnen 72 uur nadat het incident is ontdekt (*initial assessment of the incident*) en tot slot een eindverslag uiterlijk 1 maand na de incidentmelding (*final report*). Tussenin, kan het nationale CSIRT om tussentijdse verslagen verzoeken.

Het CCB heeft een uitgebreide gids ontwikkeld over wanneer en hoe een incident moet worden gemeld. De meest recente versie van de gids is beschikbaar op onze website of via deze directe link: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20NL.pdf.

NIS2-incidenten kunnen bij het CCB worden gemeld via het platform: http:https://notif.safeonweb.be/nl.

Meer informatie is ook hier beschikbaar: https://ccb.belgium.be/nl/cert/een-incident-melden.

3.3.2. Wanneer is een incident "significant"?

De NIS2-wet bevat de verplichting voor alle entiteiten binnen het toepassingsgebied om elk incident dat kan worden beschouwd als een "significant" incident te melden aan het CCB. Een significant incident wordt in de wet als volgt gedefinieerd:

"*elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:*

1. *een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of*
2. *andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.*"

Ten eerste, moet het incident gevolgen hebben voor de verlening van een van de diensten in de sectoren of deelsectoren opgesomd in bijlage I en II van de wet, d.w.z. **het moet gevolgen hebben op de netwerk- en informatiesystemen die de verlening van een of meer van deze dienst(en) ondersteunen** (bv. elektriciteitsdistributie).

De verplichte meldingen hebben daarom alleen betrekking op de informatiesystemen en -netwerken waarvan de betrokken entiteit afhankelijk is om de dienst(en) te verlenen die in de bijlagen bij de wet worden opgesomd. Een incident op een geïsoleerd informatiesysteem dat geen verband heeft met de levering van bovengenoemde diensten, hoeft dus niet te worden gemeld.

Ten tweede moeten deze gevolgen significant zijn, namelijk het incident moet minstens een van de volgende drie situaties veroorzaken of kunnen veroorzaken:

ernstige operationele storing van een van de geleverde diensten (in de sectoren of deelsectoren opgesomd in bijlagen I en II van de NIS2-wet);

- een **ernstige operationele verstoring van een van de geleverde diensten** (in de sectoren of deelsectoren opgesomd in de bijlagen I en II van de NIS2-wet);
- **financiële verliezen voor de betrokken entiteit**;
- **aanzienlijke materiële, fysieke of morele schade aan andere natuurlijke personen of rechtspersonen**.

Meer informatie over het melden van incidenten is beschikbaar in onze **Handleiding voor het melden van incidenten voor NIS2.**[3]

NIS2-incidenten kunnen worden gemeld via ons webformulier voor het melden van incidenten: https://notif.safeonweb.be/nl.

3.3.3. Ontvangers van een verplichte melding van een significant incident

In principe moet elke NIS2-entiteit een incident enkel melden aan het CCB. Het CCB stuurt de meldingen door naar de betrokken sectorale overheden en naar het crisiscentrum (voor essentiële entiteiten).

Art. 34, §1 NIS2-wet

Er is echter een uitzondering op deze regel voor entiteiten in de sector bankwezen en sector infrastructuur voor de financiële markt die onder de DORA-verordening vallen. Entiteiten in deze twee sectoren melden hun incident, naargelang het geval, bij de Nationale Bank van België (NBB) of de Autoriteit voor Financiële Diensten en Markten (FSMA), die de incidentmelding automatisch doorsturen naar het CCB.

In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van hun diensten. De entiteit deelt ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen en correcties die ontvangers kunnen nemen in reactie op die dreiging. In voorkomend geval informeren de entiteiten die ontvangers ook over de significante cyberdreiging zelf.

Art. 34, §2 NIS2-wet

3.3.4. Procedure voor het melden van incidenten

Het melden van significante incidenten gebeurt in verschillende fasen:

Art. 35 NIS2-wet

1. onverwijld en in elk geval binnen **24 uur** nadat zij kennis hebben gekregen van het significante incident, bezorgt de entiteit een vroegtijdige waarschuwing;
2. onverwijld en in elk geval binnen **72 uur** (24 uur voor verleners van vertrouwensdiensten) nadat zij kennis hebben gekregen van het significante incident, bezorgt de entiteit een incidentmelding
3. **op verzoek van** het nationale CSIRT of van de eventuele betrokken sectorale overheid, bezorgt de entiteit een tussentijds verslag;
4. uiterlijk **één maand** na de in 2. bedoelde incidentmelding stuurt de entiteit een eindverslag;
5. als het eindverslag niet kan worden verstuurd omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en vervolgens, binnen een maand na de definitieve afhandeling van het incident, het eindverslag.

In de praktijk wordt een melding van incidenten gedaan via ons platform: https://notif.safeonweb.be/nl.

---

[3] https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20NL.pdf
Zie ook de uitvoeringshandeling van de Commissie (sectie 5.1).

3.3.5. Informatie die moet worden verstrekt bij het melden van een incident

In de verschillende stadia van de melding worden verschillende soorten informatie doorgegeven:

Art. 35 NIS2-wet

- De vroegtijdige waarschuwing geeft aan of het vermoeden bestaat dat het significante incident veroorzaakt is door een onrechtmatige of kwaadwillige handeling en of het grensoverschrijdende gevolgen kan hebben. Deze vroegtijdige waarschuwing bevat alleen de informatie die nodig is om het incident onder de aandacht van het CSIRT te brengen en stelt de betrokken entiteit in staat om zo nodig om bijstand te vragen.
  Een dergelijke waarschuwing mag de middelen van de meldende entiteit niet afleiden van activiteiten op het gebied van incidentenbeheer die prioriteit zouden moeten hebben, om te voorkomen dat de meldingsplicht voor incidenten middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.
- Het doel van de incidentmelding binnen 72 uur is het actualiseren van de informatie die is gecommuniceerd als onderdeel van de vroegtijdige waarschuwing. Het biedt ook een eerste beoordeling van het incident, inclusief de ernst en de gevolgen ervan, evenals indicatoren van aantasting, indien beschikbaar.
  Net als bij vroegtijdige waarschuwing mag de melding van incidenten geen beslag leggen op de middelen van de entiteit, om te voorkomen dat de meldingsplicht middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.
- Het tussentijds verslag bevat relevante updates over de situatie.
- Het eindverslag moet een gedetailleerde beschrijving van het incident bevatten, inclusief de ernst en de gevolgen ervan; het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; de toegepaste en lopende risicobeperkende maatregelen; en in voorkomend geval, de grensoverschrijdende gevolgen van het incident.
- Het voortgangsverslag bevat zoveel mogelijk van de informatie die in het eindverslag zou moeten staan en die in het bezit is van de entiteit op het moment dat het voortgangsverslag wordt ingediend.

3.3.6. Vertrouwelijkheidsregels die van toepassing zijn op informatie die wordt doorgegeven tijdens een incident

De NIS2-entiteit en haar onderaannemers beperken de toegang tot informatie met betrekking tot incidenten, in de zin van de NIS2-wet, tot alleen die personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

Art. 26, §3-§4 NIS2-wet

Informatie die door een NIS2-entiteit aan het CCB, het NCCN en de sectorale overheid wordt verstrekt, kan worden uitgewisseld met autoriteiten in andere EU-lidstaten en met andere Belgische autoriteiten wanneer dit noodzakelijk is voor de toepassing van wettelijke bepalingen.

Deze overdracht van informatie is echter beperkt tot wat relevant en evenredig is met het doel van de uitwisseling, in overeenstemming met EU-verordening 2016/679 (AVG), de vertrouwelijkheid van de betreffende informatie en de beveiligings- en commerciële belangen van de NIS2-entiteiten.

3.4. Waar kan ik een NIS2-incident melden?

Alle NIS2-incidenten kunnen worden gemeld via ons online meldingsformulier: https://notif.safeonweb.be/nl.

Meer informatie over het melden van incidenten is te vinden op onze website.

Zie ook onze gids voor melding van incidenten voor meer informatie over "significante" incidenten.

3.5. Wat gebeurt er als er zich een incident voordoet waarbij ook persoonlijke gegevens betrokken zijn?

Zoals nu ook het geval is, gaan de meldingen van incidenten in het kader van de wet niet de eventuele meldingen bij een inbreuk in verband met persoonsgegevens vervangen, bijvoorbeeld aan de gegevensbeschermingsautoriteit (GBA). Er zullen nog steeds twee aparte meldingen nodig zijn.

De wet voorziet echter in een nauwere samenwerking tussen de nationale cyberbeveiligingsautoriteit en de gegevensbeschermingsautoriteiten. Deze samenwerking zou kunnen leiden tot de ontwikkeling van gemeenschappelijke instrumenten.

Een melding aan de Gegevensbeschermingsautoriteit (GBA) gebeurt via hun website.

3.6. Is het mogelijk om incidenten of cyberdreigingen vrijwillig te melden?

Het nationale CSIRT (CCB) kan ook, op vrijwillige basis, meldingen van incidenten, cyberdreigingen of bijna-incidenten ontvangen van entiteiten die al dan niet onder de NIS2-wet vallen.

Art. 38 NIS2-wet

Een cyberdreiging is "elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden".

Een bijna-incident is “een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan”.

Deze vrijwillige meldingen worden op dezelfde manier behandeld als verplichte meldingen. Het is echter mogelijk dat verplichte meldingen voorrang krijgen.

Een vrijwillige melding heeft niet als direct gevolg dat de meldende entiteit wordt geïnspecteerd of dat haar extraverplichtingen worden opgelegd waaraan zij niet zou zijn onderworpen als ze de melding niet had ingediend. Zie voor meer informatie de procedure die wordt uitgelegd in sectie 3.3.

3.7. Wat als mijn leverancier of een bedrijf in mijn groep een incident heeft? Wie moet dat melden? Wat als het in meerdere lidstaten gebeurt?

Elke organisatie die onder NIS2 valt en een significant incident heeft, moet dit afzonderlijk melden bij de bevoegde autoriteiten voor NIS2 in de EU. Alle andere organisaties kunnen hun incidenten ook vrijwillig melden bij het CCB via het in sectie 3.3.1 vermelde platform.

Indien het incident dat de leverancier of een ander bedrijf van de groep treft, ook een significant incident wordt voor de betrokken NIS2-entiteit, dan moet deze dit melden. NIS2-entiteiten en hun leveranciers of partnerbedrijven moeten met elkaar communiceren en elkaar informeren over cyberbeveiligingsincidenten die van invloed zijn op de levering van hun diensten.

Als het significante incident gevolgen heeft voor meerdere bedrijven (of één bedrijf) die in meerdere verschillende lidstaten zijn gevestigd, dan moet het incident worden gemeld volgens de bevoegdheidsregels zoals uitgelegd in sectie 1.14. Het is mogelijk dat het incident in bepaalde uitzonderlijke gevallen in meerdere lidstaten moet worden gemeld (bijvoorbeeld één bedrijf met één rechtspersoon die in meerdere lidstaten is gevestigd en niet alleen onder de uitzondering voor hoofdvestiging). In de praktijk heeft een incident vaak alleen gevolgen voor één lidstaat en moet de entiteit het dus in één lidstaat melden.

3.8. Wat valt er onder de twee aansprakelijkheidsregelingen van de wet (art. 31 & 61)?

Zie ook de secties 3.9 en 3.10 hieronder.

Artikel 31, § 1 van de NIS2-wet bepaalt dat bestuursorganen aansprakelijk zijn voor inbreuken op artikel 30 (cyberbeveiligingsmaatregelen) door hun entiteiten. Volgens de theorie van het orgaan wordt de aansprakelijkheid van de rechtspersoon in principe ingeschakeld door het optreden van zijn organen, zoals bepaald in artikel 2:49 van het Wetboek van vennootschappen en verenigingen.

De theorie van de cumulatieve aansprakelijkheid is echter van toepassing op de burgerlijke aansprakelijkheid, met name onder de voorwaarden en binnen de grenzen die zijn vastgesteld in de artikelen 2:56 tot 2:58 van het Wetboek van vennootschappen en verenigingen, zodat de burgerlijke aansprakelijkheid van de leden van de toezichthoudende organen (op zijn minst van de leden van de bestuursorganen) kan ontstaan op de dubbele voorwaarde dat de fout van buitencontractuele aard is en de marge waarbinnen normaal voorzichtige en zorgvuldige bestuurders zich in dezelfde omstandigheden zouden bevinden, duidelijk overschrijdt.

Bovendien stelt artikel 61, lid 1, van de NIS2-wet een specifieke aansprakelijkheid in voor elke natuurlijke persoon die verantwoordelijk is voor een essentiële of belangrijke entiteit of die optreedt als wettelijk vertegenwoordiger van een essentiële of belangrijke entiteit op grond van de bevoegdheid om deze te vertegenwoordigen, namens deze entiteit beslissingen te nemen of zeggenschap over deze entiteit uit te oefenen, op grond van hun bevoegdheid om ervoor te zorgen dat de entiteit deze wet naleeft. Dergelijke personen zijn aansprakelijk voor inbreuken op hun plicht om ervoor te zorgen dat de NIS2-wet wordt nageleefd.

Wat administratieve maatregelen betreft, staat de NIS2-wet bij herhaalde inbreuken toe dat aan elke natuurlijke persoon die leidinggevende verantwoordelijkheden uitoefent op het niveau van directeur of wettelijk vertegenwoordiger in de betrokken essentiële entiteit, tijdelijk een verbod wordt opgelegd om leidinggevende verantwoordelijkheden uit te oefenen in die entiteit, totdat de betrokken essentiële entiteit de nodige maatregelen heeft genomen om de tekortkomingen te verhelpen of om te voldoen aan de eisen van de bevoegde autoriteit die aan de oorsprong ligt van de toepassing van deze handhavingsmaatregelen (artikel 60, lid 1, 2°, en lid 2, NIS2-wet; zie ook sectie).

Tot slot kan worden opgemerkt dat de NIS2-wet de toepassing van strafrechtelijke aansprakelijkheid niet in de weg staat. De strafrechtelijke aansprakelijkheid van rechtspersonen sluit die van natuurlijke personen die dezelfde handelingen hebben gepleegd of daaraan hebben deelgenomen, niet uit.

Met uitzondering van de bepaling betreffende administratieve maatregelen, die alleen van toepassing is op essentiële entiteiten, zijn de hierboven uiteengezette elementen van toepassing op zowel essentiële als belangrijke entiteiten.

3.9. Wat zijn de verplichtingen en verantwoordelijkheden van het management?

Art. 31 & 61 NIS2-wet

De bestuursorganen van NIS2-entiteiten moeten maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren en toezien op de uitvoering ervan. Als de entiteit haar verplichtingen met betrekking tot risicobeheersmaatregelen niet nakomt, is het bestuursorgaan aansprakelijk.

Leden van bestuursorganen zijn verplicht om training te volgen om ervoor te zorgen dat hun kennis en vaardigheden voldoende zijn om risico's te identificeren en maatregelen te beoordelen voor het beheer van cyberbeveiligingsrisico's en de impact daarvan op de diensten die door de betrokken entiteit worden geleverd.

De verantwoordelijke natuurlijke personen en/of wettelijke vertegenwoordigers van een entiteit moeten de bevoegdheid hebben om ervoor te zorgen dat de entiteit de wet naleeft. Ze zijn aansprakelijk als ze dit nalaten.

Het doel van deze verantwoordingsplicht is om cyberbeveiliging te veranderen in een onderwerp dat er echt toe doet voor de betrokken entiteiten.

Deze aansprakelijkheidsregels doen geen afbreuk aan de aansprakelijkheidsregels die van toepassing zijn op publieke instellingen, noch aan de aansprakelijkheid van ambtenaren en verkozen of aangestelde ambtenaren.

Natuurlijke personen die leidinggevende functies uitoefenen op het niveau van directeur of wettelijk vertegenwoordiger in een NIS2-entiteit kunnen tijdelijk worden uitgesloten van het uitoefenen van leidinggevende verantwoordelijkheden in deze entiteit, in geval van schending van de vereisten van de NIS2-wet.

3.10. Wat is een "bestuursorgaan"?

Het begrip "bestuursorgaan" is niet gedefinieerd in de richtlijn.

De memorie van toelichting bij de NIS2-wet definieert "lid van een bestuursorgaan" als volgt:

Iedere natuurlijke of rechtspersoon die :

(i) een functie uitoefent binnen of in verband met een entiteit die hem of haar in staat stelt (a) die entiteit te beheren en te vertegenwoordigen of (b) namens en voor rekening van die entiteit beslissingen te nemen die juridisch bindend zijn voor die entiteit of deel te nemen, binnen een orgaan van die entiteit, aan besluitvorming over dergelijke beslissingen, of

(ii) controle uitoefent over de entiteit, zijnde de bevoegdheid in rechte of in feite om een beslissende invloed uit te oefenen op de aanstelling van een meerderheid van de bestuurders of zaakvoerders of op de oriëntatie van het beleid.

Indien de entiteit in kwestie een vennootschap naar Belgisch recht is, wordt deze controle bepaald overeenkomstig artikel 1:14 tot 1:18 van het Wetboek van vennootschappen en verenigingen.

Wanneer de persoon wiens rol wordt onderzocht, een rechtspersoon is, wordt het begrip "lid van een bestuursorgaan" terugwerkend onderzocht en omvat het zowel de rechtspersoon in kwestie als elk lid van een bestuursorgaan van die rechtspersoon.

3.11. Wat moet de inhoud zijn van de training voor het management?

Het doel van de opleiding voor leden van het bestuursorgaan is om hen in staat te stellen de taken die hen bij wet zijn toegewezen correct uit te voeren, d.w.z. maatregelen voor het beheer van cyberbeveiligingsrisico's goed te keuren en toezicht te houden op de uitvoering van deze maatregelen. De exacte opleidingsvereisten worden niet vermeld. De inhoud en duur van de opleiding worden daarom aan de entiteiten overgelaten.

Ons CyberFundamentals Framework bevat informatie over het opleidingsproces, met name wat betreft inhoud en doelgroep. Bijvoorbeeld, voor het zekerheidsniveau 'belangrijk' is het gedeelte over training te vinden vanaf pagina 28 (CyFun® 2023).

Als toezichthoudende autoriteit kan het CCB geen trainingen aanbieden voor NIS2-entiteiten, noch kunnen we specifieke trainingsprogramma's aanraden.

3.12. Wat zijn de wettelijke voorwaarden om gebruik te maken van het beschermend kader bij het onderzoeken en rapporteren van kwetsbaarheden (ethisch hacken)?

Art. 22 en 23 NIS2-wet

De NIS2-wet bevat de bepalingen van de NIS1-wet, die een beschermend kader (*safe harbour)* biedt voor "ethische hackers" of "digitale klokkenluiders".

Om van dit kader te kunnen profiteren, moet de persoon:

- Handelen zonder bedrieglijk opzet of het oogmerk om te schaden;
- Binnen 24 uur na de ontdekking van de kwetsbaarheid een vereenvoudigde melding naar zowel het nationale CSIRT als de verantwoordelijke organisatie sturen;
- Binnen 72 uur na de ontdekking een volledige kennisgeving sturen naar dezelfde ontvangers;
- Zich onthouden van verder te gaan dan wat nodig en evenredig is om het bestaan van een kwetsbaarheid na te gaan en te melden;
- Zich onthouden een kwetsbaarheid openbaar te maken zonder toestemming van het nationale CSIRT.

Bovendien moeten ethische hackers om kwetsbaarheden te kunnen onderzoeken op netwerk- en informatiesystemen van bepaalde organisaties (zoals inlichtingendiensten, defensie, rechterlijke instanties.) en de informatie die door hen of namens hen wordt verwerkt, voorafgaandelijk een schriftelijke overeenkomst sluiten met deze organisaties.

Op haar website biedt het CCB algemene informatie over ethisch hacken aan met inbegrip van een pagina gewijd aan de bekendmaking van kwetsbaarheden.

3.13. Wat zijn de registratieverplichtingen?

3.13.1. Hoe registreren NIS2-entiteiten zich?

Essentiële en belangrijke entiteiten moeten zich registreren op het CCB-portaal, Safeonweb@Work.

Art. 13 NIS2-wet

De termijn voor registratie hangt af van het type entiteit. In principe hebben essentiële en belangrijke entiteiten, evenals entiteiten die domeinnaamregistratiediensten verlenen, **5 maanden de tijd** om zich te registreren nadat de wet in werking is getreden, d.w.z. uiterlijk **18 maart 2025**. Bij de registratie moeten zij de volgende informatie verstrekken:

1. hun naam en hun registratienummer bij de KBO of een gelijkwaardige inschrijving in de Europese Unie;
2. hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereiken en hun telefoonnummer;
3. indien van toepassing, de relevante sector en deelsector bedoeld in bijlage I of II van de wet;
4. indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen

Er bestaat een uitzondering voor entiteiten die deze informatie al hebben doorgegeven aan een NIS2 sectorale overheid op grond van een wettelijke verplichting. In dit geval hoeft de informatie alleen maar te worden aangevuld bij autoriteit. Als de informatie verandert, moet dit binnen twee weken worden doorgegeven.

Voor de volgende types entiteiten bestaat een licht aangepaste regeling:

Art. 14 NIS2-wet

- DNS-dienstverleners;
- registers voor topleveldomeinnamen;

- entiteiten die domeinnaamregistratiediensten verlenen;
- aanbieders van cloudcomputingdiensten;
- aanbieders van datacentrumdiensten;
- aanbieders van netwerken voor de levering van inhoud;
- aanbieders van beheerde diensten;
- aanbieders van beheerde beveiligingsdiensten;
- aanbieders van onlinemarktplaatsen;
- aanbieders van onlinezoekmachines;
- aanbieders van platformen voor socialenetwerkdiensten.

Zij moeten zich binnen **2 maanden** na de inwerkingtreding van de wet, d.w.z. uiterlijk **18 december 2024**, registreren en de volgende informatie verstrekken:

1. hun naam;
2. hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;
3. het adres van hun hoofdvestiging en hun andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van hun vertegenwoordiger;
4. hun actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers en, indien van toepassing van hun vertegenwoordiger;
5. de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren;
6. hun IP-bereiken.

Ook hier is elke entiteit verplicht om het CCB onmiddellijk op de hoogte te stellen van wijzigingen in hun informatie.

In de praktijk wordt een deel van deze informatie rechtstreeks van de Kruispuntbank van Ondernemingen (KBO) verkregen tijdens het registratieproces.

3.13.2. Hoe kan ik mijn organisatie registreren?

Alle praktische details met betrekking tot de registratieprocedure worden uitgelegd in onze NIS2-registratiegids die online beschikbaar is.

In het kort: de wettelijke vertegenwoordigers van een organisatie die vermeld staat in de Kruispuntbank van Ondernemingen (KBO) (zoek uw organisatie hier op) kunnen zichzelf aansluiten op het My eGov-rollenbeheer platform om de nodige autorisaties te verlenen aan elke geschikte Belgische burger om een organisatie te registreren op ons Safeonweb@Work platform. Alle informatie is beschikbaar in de gids.

3.13.3. Hoe weet ik of mijn organisatie al geregistreerd is?

De persoon vermeld in sectie 3.13.2 moet zichzelf aanmelden op het platform om dit te verifiëren.

3.13.4. Welke entiteiten moeten zich registreren in een groep bedrijven? Kan alleen de holding zich registreren?

Binnen een groep bedrijven **moeten** alle organisaties/afzonderlijke juridische entiteiten (zelfs mogelijk de holding - afhankelijk van de geleverde diensten) die onder NIS2 **vallen, zich**

afzonderlijk registreren. Het bedrijf kan zich niet in plaats van de bedrijven in zijn groep registreren.

3.13.5. Wat als mijn organisatie afdelingen of subentiteiten heeft die verschillende types entiteiten zijn?

Als deze afdelingen of subentiteiten allemaal deel uitmaken van dezelfde juridische entiteit, dan moet deze juridische entiteit zich laten registreren onder de verschillende types entiteiten (sectoren) waaronder het kwalificeert onder de NIS2-wet.

Als de verschillende subentiteiten afzonderlijke juridische entiteiten zijn die allemaal als "entiteit" kunnen worden aangemerkt onder NIS2 (zie sectie 1.4), dan kunnen ze zich allemaal afzonderlijk registreren.

3.13.6. Moeten organisaties in de toeleveringsketen van NIS2-entiteiten zich registreren?

Alleen organisaties die onder het toepassingsgebied van NIS2 vallen, moeten zich registreren. Het is mogelijk dat organisaties in de toeleveringsketen van NIS2-entiteiten zelf geen NIS2-entiteiten zijn en zich dus niet hoeven te registreren.

Voor meer informatie over de toeleveringsketen, zie sectie 3.14.

3.13.7. Hoe kan een buiten België gevestigde organisatie zich registreren? Hoe kan een wettelijke vertegenwoordiger een organisatie registreren?

Er zijn twee uitzonderlijke situaties waarin organisaties buiten België zich moeten registreren:

1) Zij leveren elektronische-communicatienetwerken of -netwerken in België (zie sectie 1.14);
2) Ze vallen onder het regime van de hoofdvestiging (zie sectie 1.14), zijn buiten de EU gevestigd, verlenen diensten in België, kozen België als hun plaats van registratie in de EU en wijzen er een wettelijke vertegenwoordiger aan.

In deze twee situaties, als organisaties zich niet kunnen registreren via de Safeonweb@Work-website, moeten ze contact opnemen met het CCB via info@ccb.belgium.be.

3.13.8. Moet ik me opnieuw registreren als mijn organisatie al onder NIS1 viel?

Ja, de organisatie moet zich opnieuw registreren.

3.13.9. Hoe kan ik bewijzen dat mijn organisatie is geregistreerd?

NIS2-organisaties kunnen het CCB via info@ccb.belgium.be vragen om een document als bewijs van hun registratie.

Dit handmatige proces wordt binnenkort vervangen door een downloadbaar document op het platform.

3.13.10. Wat gaat het CCB doen met organisaties die zich niet registreren?

Het CCB zal, op basis van de informatie waarover het als federale overheidsinstantie beschikt, proactief proberen entiteiten op te sporen en te benaderen die zich niet hebben geregistreerd. Het is belangrijk om op te merken dat entiteiten die zich niet hebben geregistreerd, kunnen worden gezien als het schenden van de NIS2-wet en zichzelf mogelijk blootstellen aan passende administratieve maatregelen en boetes.

3.14. Supply chain: Hoe kan een entiteit de relaties met haar leveranciers en directe dienstverleners beheren ?

Als onderdeel van de minimumlijst van maatregelen voor het beheer van cyberbeveiligingsrisico's moeten entiteiten die onder de NIS2-wet vallen passende en evenredige maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen.

Art. 30, §3, 4° NIS2-wet

Een van deze maatregelen is de beveiliging van de toeleveringsketen van de entiteit. Dit omvat de beveiligingsaspecten van de relatie tussen elke entiteit en haar **directe leveranciers of dienstverleners**.

De gevolgen van deze verplichting zijn vanuit twee invalshoeken voelbaar: Het houdt niet alleen in dat NIS2-entiteiten maatregelen voor het beheer van cyberbeveiligingsrisico's moeten opleggen aan de organisaties in hun toeleveringsketen(s) (zoals leveranciers en onderaannemers) en toezicht op hen moeten houden, maar ook dat entiteiten die niet binnen het toepassingsgebied van NIS2 vallen, ook passende en evenredige maatregelen voor het beheer van cyberbeveiligingsrisico's moeten nemen.

De NIS2-wet geeft niet aan hoe NIS2-entiteiten moeten omgaan met de directe toeleveringsketenverplichting. Het wordt met name aan de entiteiten zelf overgelaten om te controleren of de organisaties in hun toeleveringsketen hun verplichtingen nakomen. Het CCB raadt alle NIS2-entiteiten aan om de organisaties in hun toeleveringsketen contractueel een label of certificering op te leggen, zoals opgenomen in het CyberFundamentals (CyFun®) Framework, om het aantonen van naleving van de toeleveringsketenverplichting te vergemakkelijken.

Voor lopende contracten met leveranciers en dienstverleners is het de verantwoordelijkheid van de entiteit om de momenteel geldende bepalingen te beoordelen en ervoor te zorgen dat ze voldoen aan de verplichtingen. Het is mogelijk dat bestaande contracten moeten worden herzien. De NIS2-entiteit moet voldoende contractuele waarborgen inbouwen voor het geval de organisatie in haar toeleveringsketenverplichting niet nakomt. Zie de tijdlijn in sectie 4.14 om na te gaan wanneer de contracten moeten worden aangepast.

Om het juiste CyFun®-zekerheidsniveau voor leveranciers en dienstverleners te kiezen, moet het NIS2 een risicobeoordeling uitvoeren en op basis van het resultaat het meest geschikte niveau opleggen. Hiervoor kan de CyFun® Risk Assessment tool worden gebruikt.

Voor alle entiteiten die niet onder het toepassingsgebied van de NIS2-wet vallen, raadt het CCB aan om ook passende en evenredige maatregelen te nemen voor het beheer van cyberbeveiligingsrisico's om zich voor te bereiden op het geval dat zij deel uitmaken van de toeleveringsketen van een NIS2-entiteit. Ook hier kunnen ze een beroep doen op het CyFun® Framework om de concrete maatregelen die ze zouden kunnen moeten nemen te identificeren en te implementeren.

Noch een bepaald eigenaarschap van de NIS2-entiteit van een organisatie in haar toeleveringsketen, noch de omvang van laatstgenoemde hebben invloed op het toepassingsgebied van deze verplichting. Dit element kan enkel mogelijks van invloed zijn op de risicobeoordeling van de toeleveringsketen van de NIS2-entiteit.

Zie sectie 3.7 voor de behandelen van incidenten bij leveranciers. Zie ook sectie 3.9 over de verantwoordelijkheid van bestuursorganen voor maatregelen voor het beheer van cyberbeveiligingsrisico's.

3.15. Welke vertrouwelijkheidsverplichtingen moeten worden gerespecteerd?

Art. 26 NIS2-wet

De bevoegde autoriteiten, essentiële en belangrijke entiteiten en hun onderaannemers beperken de toegang tot informatie in het kader van de NIS2-wet tot personen die deze informatie nodig hebben en tot degenen die er toegang toe hebben om hun functies of taken in verband met de uitvoering van de wet uit te voeren.

Informatie die door essentiële en belangrijke entiteiten aan de bevoegde autoriteiten wordt verstrekt, kan niettemin worden uitgewisseld met autoriteiten in de Europese Unie, met Belgische autoriteiten of met buitenlandse autoriteiten, indien dit noodzakelijk is voor de toepassing van wettelijke bepalingen.

De uitgewisselde informatie is beperkt tot wat relevant en evenredig is voor het doel van de uitwisseling, in het bijzonder in overeenstemming met Verordening (EU) 2016/679 (AVG). Deze uitwisseling van informatie bewaart de vertrouwelijkheid van de betrokken informatie en beschermt de veiligheid en commerciële belangen van essentiële en belangrijke entiteiten.

Art. 27 NIS2-wet

De wet staat echter de vrijwillige uitwisseling van relevante informatie over cyberbeveiliging toe, met name informatie over cyberbedreigingen, vermeden incidenten, bijna-incidenten, kwetsbaarheden, enz. Deze uitwisseling vindt onder bepaalde voorwaarden plaats in het kader van gemeenschappen voor informatie-uitwisseling, uitgevoerd door middel van overeenkomsten voor informatie-uitwisseling.

4. Controle / Toezicht

4.1. Wie worden de bevoegde autoriteiten?

Art. 15, 16 e.v. NIS2-wet en art. 3 KB NIS2

4.1.1. Centrum voor Cybersecurity België (CCB)

De nationale cyberbeveiligingsautoriteit (CCB) is verantwoordelijk voor de opvolging, de coördinatie van en het toezicht op de wet. Daartoe combineert de wet de bestaande taken van het CCB met de aanvullingen van de NIS2-richtlijn, met name wat betreft het toezicht op entiteiten. Het CCB is verantwoordelijk voor het toezicht op essentiële en belangrijke entiteiten (met de hulp van de sectorale overheden) en is het centrale contactpunt voor de implementatie van NIS2.

Het nationale Computer Security Incident Response team (CSIRT) maakt ook deel uit van de nationale cyberbeveiligingsautoriteit. NIS2-entiteiten zijn verplicht significante incidenten aan dit CSIRT te melden.

4.1.2. Sectorale overheden

De volgende sectorale overheden zijn aangewezen:

1. **voor de sector energie**: de federale minister bevoegd voor Energie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
2. **voor de sector vervoer**:
    a. Wat betreft de sector vervoer, met uitzondering van het vervoer over water: de federale minister bevoegd voor Vervoer of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
    b. Wat betreft het vervoer over water: de federale minister bevoegd voor Maritieme Mobiliteit of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
3. **voor de sector gezondheidszorg**:
    a. wat betreft entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen; entiteiten die farmaceutische basisproducten en farmaceutische preparaten vervaardigen; en entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG);
    b. de federale minister bevoegd voor Volksgezondheid of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
4. **voor de sector digitale infrastructuur:** Belgisch Instituut voor postdiensten en telecommunicatie (BIPT);

5. **voor wat betreft de verleners van vertrouwensdiensten**: e federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
6. **voor de sector digitale aanbieders**: de federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
7. **voor de sector ruimtevaart en de sector onderzoek**: de federale minister van Wetenschapsbeleid of bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
8. **voor drinkwater**: het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater
9. **voor de sector bankwezen**: de Nationale Bank van België (NBB);
10. **voor de sector infrastructuur voor de financiële markt**: de Autoriteit voor Financiële Diensten en Markten (FSMA);
11. **voor de deelsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek**: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten.

Sectorale overheden hebben een aantal bevoegdheden. Voor meer informatie, zie sectie 4.8.

Entiteiten die onder een sectorale overheid vallen, kunnen er terecht voor informatie, bijstand, enz.

4.1.3. Het Nationaal Crisiscentrum (NCCN)

Het Nationaal Crisiscentrum is ook betrokken bij de implementatie van de NIS2-wet, met name wat betreft de melding van incidenten, cybercrisisbeheer en de fysieke beveiligingsmaatregelen die worden genomen door exploitanten van kritieke infrastructuur en kritieke entiteiten (die onder de CER-richtlijn vallen).

4.2. Welke referentiekaders kunnen door NIS2-entiteiten worden gebruikt om hun conformiteit aan te tonen?

Essentiële entiteiten die onderworpen zijn aan de verplichting tot regelmatige conformiteitsbeoordeling kunnen ervoor kiezen om een van de twee referentiekaders te gebruiken die in het koninklijk besluit NIS2 worden genoemd.

Art. 5, §1 NIS2 koninklijk besluit

Het gebruik van deze referentiekaders voor controle wordt uitgelegd in de volgend sectie (4.4).

4.2.1. Het CyberFundamentals Framework (CyFun®)

Het CyberFundamentals (CyFun®) Framework[4] is een reeks concrete maatregelen om:

- gegevens te beschermen;
- het risico op de meest voorkomende cyberaanvallen aanzienlijk te verkleinen;
- de cyberweerbaarheid van een organisatie te vergroten.

[4] https://cyfun.be

Om te reageren op de ernst van de bedreiging waaraan een organisatie wordt blootgesteld, worden naast het startniveau Small, drie zekerheidsniveaus geboden: Basic, Important en Essential. De framework werd gevalideerd met behulp van CERT-aanvalsprofielen (verkregen uit succesvolle aanvallen). De conclusie is dat:

- maatregelen op zekerheidsniveau Basic 82% van de aanvallen kunnen dekken;
- maatregelen op zekerheidsniveau Important 94 % van de aanvallen kunnen dekken;
- maatregelen op zekerheidsniveau Essential 100% van de aanvallen kunnen dekken.

Daarnaast is het CyFun® Framework:

- **gebaseerd op erkende standaarden**: CyFun® selecteert relevante controles op basis van gangbare standaarden zoals NIST CSF, ISO/IEC 27001, CIS Controls en IEC 62443;
- **overeengekomen met de maatregelen die nodig zijn** om de belangrijkste door het CCB geïdentificeerde aanvallen te voorkomen;
- **door iedereen te gebruiken**: elke controle gaat gepaard met richtlijnen om de implementatie te ondersteunen. CyFun®'s self-assessment-tool helpt om een overzicht over de implementatie te behouden;
- **nuttig bij de validering van je implementatie**: de implementatie kan worden gevalideerd door een beoordeling aan te vragen bij een erkende conformiteitsbeoordelingsinstantie. Dit attest geeft je klanten en overheden het bewijs van je implementatie (bv. om te voldoen aan NIS2).

In de context van NIS2 is het CyFun® Framework een handig hulpmiddel, niet alleen voor essentiële entiteiten die onderworpen zijn aan een regelmatige conformiteitsbeoordeling, maar ook voor belangrijke entiteiten. Het is gratis beschikbaar en biedt eenvoudige oplossingen voor risicobeoordeling, zelfbeoordeling en voor het invoeren van de minimale door de NIS2-wet vereiste maatregelen voor het beheer van cyberbeveiligingsrisico's. Bovendien geeft een gevalideerde of gecertificeerde implementatie van het CyFun® Framework de betrokken entiteiten een vermoeden van conformiteit in het kader van het toezicht onder NIS2.

Het CCB raadt alle NIS2-entiteiten aan het CyFun® Framework te gebruiken, dat openbaar en gratis beschikbaar is op onze Safeonweb@Work-website.

4.2.2. ISO/IEC 27001

De Europese norm ISO/IEC 27001 is een internationaal erkende technische norm die de algemene en gestructureerde aanpak beschrijft voor het beveiligingsbeheer van elk informatiesysteem. Ze is daarom een basisnorm die de algemene principes uiteenzet voor het implementeren van beveiligingsmaatregelen voor informatiesystemen en ze is van toepassing op alle sectoren.

De laatste versie dateert van 2022, maar ze is zonder datumaanduiding in het koninklijk besluit opgenomen, zodat de meest recente versie altijd kan worden toegepast.

Meer informatie is te vinden op de officiële website.

4.3. Waar kan ik meer informatie vinden over CyFun®?

Alle informatie, documenten, richtsnoeren, enz. zijn gecentraliseerd op https://cyfun.be.

CyFun® heeft ook zijn eigen FAQ beschikbaar op: https://atwork.safeonweb.be/nl/cyberfundamentals-frequently-asked-questions-faq

4.4. Hoe worden de betrokken entiteiten gecontroleerd? Doet het CCB CyFun-certificeringen?

Art. 39 e.v. NIS2-wet
Art. 6-13 NIS2 koninklijk besluit

Wanneer we het hebben over controle/toezicht in de context van de wet, moeten we onderscheid maken tussen twee categorieën entiteiten: essentiële entiteiten en belangrijke entiteiten.

Essentiële entiteiten zijn verplicht een regelmatige conformiteitsbeoordeling te ondergaan. Deze beoordeling wordt uitgevoerd op basis van een keuze die de entiteit maakt uit drie opties:

- Ofwel een CyberFundamentals (CyFun®) certificering toegekend door een conformiteitsbeoordelingsinstantie (CAB) erkend door het CCB (na accreditatie door BELAC);
- of een ISO/IEC 27001-certificering, afgegeven door een CAB dat is geaccrediteerd door een accreditatie-instelling die de overeenkomst inzake wederzijdse erkenning (MLA) voor de ISO/IEC 27001-norm in het kader van de Europese samenwerking voor accreditatie (EA) of het International Accreditation Forum (IAF) heeft ondertekend en is erkend door het CCB;
- of een inspectie door de inspectiedienst van het CCB (of door een sectorale inspectiedienst).

De inspectiedienst kan ook op elk moment essentiële entiteiten controleren (zonder incident - *ex ante* - en na een incident of bij voldoende bewijs van niet-naleving van de wet - *ex post*).

Voor belangrijke entiteiten wordt het toezicht alleen "*ex post*" uitgevoerd door de inspectiedienst, d.w.z. na een incident of in het licht van bewijzen, aanwijzingen of informatie dat een belangrijke entiteit haar verplichtingen niet nakomt (art. 48, §2 van de NIS2-wet). In principe zijn ze daarom niet onderworpen aan regelmatige conformiteitsbeoordeling. Deze entiteiten kunnen zich echter vrijwillig onderwerpen aan hetzelfde regime als essentiële entiteiten.

Zie sectie voor meer informatie over de inspectie door de inspectiedienst.

Het CCB doet geen regelmatige conformiteitsbeoordelingen van NIS2-entiteiten die kunnen leiden tot een vermoeden van conformiteit, en geeft daarom ook geen CyFun®-certificaten uit. Alleen CAB's mogen dit doen.

4.5. Moet een organisatie een CyFun® certificering of verificatie krijgen als het ISO/IEC 27001 wil gebruiken?

Nee, een CyFun® certificering of verificatie is geen noodzakelijke tussenstap om een ISO/IEC 27001 certificering te ontvangen.

Het is echter mogelijk om een CyFun-label te verkrijgen door gebruik te maken van een bestaande ISO/IEC 27001-certificering met het juiste toepassingsgebied en *Statement of Applicability*.

Hiervoor moeten de benodigde documenten worden geüpload via het tabblad "Labels" op het dashboard van uw geregistreerde organisatie op Safeonweb@Work.

4.6. Wat is een conformiteitsbeoordelingsinstantie (CAB)?

Een conformiteitsbeoordelingsinstantie (CAB) is een instantie die verantwoordelijk is voor het controleren en certificeren van de naleving van de in het CyFun®-referentiekader of de ISO/IEC 27001-norm vastgestelde eisen (toegepast onder de NIS2-wet) door NIS2-entiteiten die onderworpen zijn aan regelmatige conformiteitsbeoordeling (verplicht voor essentiële entiteiten, vrijwillig voor belangrijke entiteiten).

Voor CyFun® is het geaccrediteerd door de Belgische accreditatie-instantie (BELAC) en erkend door het CCB. Voor ISO/IEC 27001 is het geaccrediteerd door een accreditatie-instelling die de Mutual Recognition Agreement (MLA) voor de ISO/IEC 27001-norm heeft ondertekend in het kader van de European co-operation for Accreditation (EA) of het International Accreditation Forum (IAF) en erkend door het CCB. Meer informatie is te vinden in de autorisatievoorwaarden voor CAB's op onze website.

4.7. Waar kan ik meer informatie vinden over CAB's?

Alle informatie met betrekking tot accreditatie in België is beschikbaar op de officiële website van BELAC: https://economie.fgov.be/nl/themas/kwaliteit-veiligheid/accreditatie.

Aanvullende informatie voor CAB's onder CyFun® is beschikbaar op onze website: https://atwork.safeonweb.be/nl/conformiteitsbeoordelingsinstanties-cab.

4.8. Wat zijn de missies van de sectorale overheden?

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 en 52 NIS2-wet

De sectorale overheden spelen ook een rol in het kader van de NIS2-wet, vanwege hun specifieke kennis en deskundigheid in elk van de betrokken sectoren. Waar nodig kunnen zij worden betrokken bij de volgende taken:

- Aanvullende identificatie (raadplegen en voorstellen);
- Registratie van entiteiten;
- Organisatie van sectorale oefeningen;
- De gevolgen van een incident voor een sector analyseren en beheren;
- Deelname aan bepaalde werkzaamheden van de NIS samenwerkingsgroep;
- Bewustmaking van entiteiten in hun sector;
- Samenwerking op nationaal niveau;
- Bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's;
- Melding van incidenten (doorgifte van de melding van significante incidenten aan de sectorale overheden, raadpleging bij verschillende situaties met betrekking tot dit onderwerp);
- Toezicht en inspectie (gezamenlijk of gedelegeerd);
- Administratieve geldboetes.

4.9. Hoe kan een entiteit bewijzen dat ze haar verplichtingen nakomt? Wat is een vermoeden van conformiteit?

Art. 42 NIS2-wet
Art. 5, §1 NIS2 koninklijk besluit

Als onderdeel van de regelmatige conformiteitsbeoordeling - die verplicht is voor essentiële entiteiten - zal de entiteit een certificering of een label kunnen krijgen, waardoor, tot bewijs van het tegendeel, kan worden vermoed dat de entiteit voldoet aan haar verplichtingen op het gebied van cyberbeveiliging.

Deze certificering zal gebaseerd zijn op de twee frameworks die in het koninklijk besluit worden genoemd: de CyberFundamentals of de internationale norm ISO/IEC 27001 (met het juiste toepassingsgebied en *Statement of Applicability*). Zie ook sectie .

Het is belangrijk op te merken dat het **toepassingsgebied** van een certificering identiek moet zijn aan het toepassingsgebied van de NIS2-wet, wat betekent dat het de netwerk- en informatiesystemen van een organisatie moet omvatten als een geheel, anders zal de certificering een organisatie niet in staat stellen gebruik te maken van een vermoeden van conformiteit.

Uiteraard kan een entiteit ook een ander referentiekader of een andere technische norm gebruiken om haar wettelijke cyberbeveiligingseisen te implementeren. In dat geval geldt het vermoeden van conformiteit niet en moet de entiteit aan de inspectiedienst aantonen dat zij alle vereiste maatregelen toepast, op basis van een concordantietabel (*mapping*) met een van de twee bovengenoemde referentiekaders.

4.10. Kun je het toepassingsgebied van een certificering of verificatie beperken tot alleen de NIS2-gerelateerde diensten en activiteiten?

Zoals opgemerkt in sectie , mag het toepassingsgebied van een certificering of verificatie niet kleiner zijn dan het toepassingsgebied van de NIS2-wet, die de hele organisatie bestrijkt.

4.11. Kan een entiteit een CyFun®-zekerheidsniveau gebruiken dat lager is dan het niveau dat aan haar entiteitscategorie is toegewezen? Verandert dat de NIS2-kwalificatie?

Art. 7 KB NIS2

Het koninklijk besluit laat een entiteit toe om een lager CyFun®-niveau te gebruiken (bijvoorbeeld het gebruik van het zekerheidsniveau Important voor een essentiële entiteit) op voorwaarde dat ze dit objectief kan rechtvaardigen op basis van haar risicoanalyse. Deze keuze blijft de exclusieve volledige verantwoordelijkheid van de entiteit in kwestie en **heeft geen invloed op haar wettelijke kwalificatie als een essentiële of belangrijke entiteit**. Er moet worden benadrukt dat deze keuze op elk moment in vraag kan worden gesteld door de inspectiedienst in het kader van zijn controleopdrachten.

Het CCB biedt een tool voor risicobeoordeling aan op Safeonweb@Work zodat een entiteit een geïnformeerde keuze kan maken over CyFun® zekerheidsniveau dat zij nodig heeft.

4.12. Hebben organisaties de toestemming van het CCB nodig om een lager niveau van CyFun® te gebruiken?

Nee, NIS2-entiteiten hoeven het CCB niet te vragen hun analyse te bevestigen om een lager niveau van CyFun® te gebruiken. Zoals aangegeven in sectie 4.11 is elke NIS2-entiteit zelf verantwoordelijk voor die keuze. De rechtvaardiging voor deze keuze moet alleen intern worden gedocumenteerd.

Tijdens een inspectie kan de relevante inspectiedienst de keuze van de entiteit controleren.

4.13. Kan een entiteit die een aanbieder van essentiële diensten (AED) uitmaakte onder NIS1 haar ISO27001-certificering behouden?

Art. 8, 12 en 14-15 KB NIS2

Als een entiteit die onder NIS1 een aanbieder van essentiële diensten (AED) uitmaakte, een ISO/IEC 27001-certificering heeft, kan hij zijn certificering gebruiken als onderdeel van een periodieke conformiteitsbeoordeling in het kader van NIS2. Indien nodig moet het toepassingsgebied van de certificering worden uitgebreid om ervoor te zorgen dat deze alle netwerk- en informatiesystemen van de betreffende entiteit omvat.

De certificering moet worden uitgevoerd door een conformiteitsbeoordelingsinstantie die is geaccrediteerd door BELAC in België (of door een andere geaccrediteerde nationale Europese instantie als deze certificering afkomstig is uit een andere lidstaat) en die is geautoriseerd door het CCB.

4.14. [Tijdlijn] Wanneer moeten de betrokken entiteiten de verplichtingen van de wet toepassen?

Art. 13 & 75 NIS2-wet

Art. 22-23 NIS2 koninklijk besluit

De meeste bepalingen uit het wettelijke kader van NIS2 treden in werking op 18 oktober 2024. Voor de uitvoering van sommige verplichtingen geeft de wet of het koninklijk besluit entiteiten echter meer tijd.

Vanaf 18 oktober 2024 zijn met name de volgende verplichtingen onmiddellijk van toepassing:

- het nemen van de minimale maatregelen voor het beheer van cyberbeveiligingsrisico's;
- het melden van alle significante incidenten;
- zich onderwerpen aan het toezicht en samenwerken met bevoegde overheden;
- voor bestuursorganen: maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren, toezicht houden op de uitvoering van maatregelen, aansprakelijkheid voor overtredingen door de entiteit en het volgen van cyberbeveiligingsopleidingen.

Voor de registratie van entiteiten bij het CCB via Safeonweb@Work voorziet de wet in deadlines:

- entiteiten die diensten verlenen die onder de digitale sectoren van de bijlagen vallen, hebben twee maanden de tijd vanaf 18 oktober 2024 om zich te registreren (**uiterlijk tot 18 december 2024**) (lijst in art. 14, §1 van de wet);
- alle andere entiteiten hebben vijf maanden de tijd vanaf 18 oktober 2024 om zich te registreren (**uiterlijk tot 18 maart 2025**).

Het toezicht/de regelmatige conformiteitsbeoordeling van essentiële entiteiten verlopen ook stapsgewijs:

- Voor het CyberFundamentals (CyFun®) Framework:
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Basic**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om een verificatie te verkrijgen door een geaccrediteerde en erkende conformiteitsbeoordelingsinstantie (hierna "CAB");
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Important**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om ofwel een Basic of een Important verificatie te verkrijgen door een geaccrediteerde en erkende CAB.
    Indien nodig kunnen zij een eerste verificatie op niveau Basic verkrijgen en na nog eens 12 maanden een verificatie op niveau Important (**uiterlijk op 18 april 2027**);
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Essential**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om ofwel een Basic of een Important verificatie te verkrijgen door een geaccrediteerde en erkende CAB.
    Ze hebben een extra deadline van 12 maanden (**uiterlijk op 18 april 2027**) waarbinnen ze een zekerheidsniveau Essential certificering moeten verkrijgen door een geaccrediteerde en erkende CAB.
- Entiteiten die kiezen voor ISO/IEC 27001-certificatie, moeten hun toepassingsgebied en *statement of applicability* **uiterlijk op 18 april 2026** indienen bij het CCB **en op uiterlijk 18 april 2027** door een CAB gecertificeerd zijn.
- Entiteiten die ervoor kiezen om rechtstreeks door het CCB te worden geïnspecteerd:
  - **Uiterlijk op 18 april 2026**: hun zelfbeoordeling van CyFun® zekerheidsniveau Basic of Important, of hun ISO/IEC 27001-informatiebeveiligingsbeleid, toepassingsgebied en *statement of applicability* aan het CCB overmaken.
  - **Uiterlijk op 18 april 2027**: verslag over de voortgang m.b.t. de conformiteit.

Belangrijke entiteiten zijn niet onderworpen aan een verplichte regelmatige conformiteitsbeoordeling (toezicht *ex-post*). Om ervoor te zorgen dat de cyberbeveiligingsmaatregelen passend en evenredig zijn, zal de inspectiedienst toezicht houden op belangrijke entiteiten, met inachtneming van een vergelijkbare periode van 18 maanden na de inwerkingtreding van de wet (om hen in staat te stellen volledig het vereiste niveau te bereiken).

Als zich bijvoorbeeld begin 2025 een significant cyberincident voordoet, zal de betrokken entiteit de nodige maatregelen moeten nemen om dit te beheren en aan het CCB te melden, mogelijk onder toezicht van de bevoegde inspectiediensten. We moedigen alle NIS2-entiteiten daarom aan om niet te wachten tot de registratiedeadline en hun eerste conformiteitsbeoordelingen om de vereiste maatregelen te implementeren.

4.15. Hoe worden inspecties uitgevoerd?

Art. 44 e.v. NIS2-wet

De inspectiedienst van de nationale cyberbeveiligingsautoriteit is bevoegd om inspecties uit te voeren om te controleren of essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

Inspecties met betrekking tot essentiële entiteiten kunnen zowel *ex ante* (voorafgaan) als *ex post* (achteraf) worden uitgevoerd. Ze worden uitgevoerd door de inspectiedienst van de nationale cyberbeveiligingsautoriteit of door de aangewezen sectorale inspectiedienst (specifieke/bijkomende sectorale maatregelen). Deze inspecties kunnen, op verzoek van de sectorale overheid, gezamenlijk worden uitgevoerd door voornoemde autoriteiten.

Essentiële entiteiten moeten ook regelmatige conformiteitsbeoordelingen ondergaan. Belangrijke entiteiten kunnen ook vrijwillig een conformiteitsbeoordeling ondergaan op basis van ISO/IEC 27001 of CyberFundamentals (zie sectie 4.4).

Inspecties *ex post* van belangrijke entiteiten worden uitgevoerd op basis van indicatoren, zoals het zich voordoen van een incident of objectief bewijs van mogelijke tekortkomingen. Ook deze inspectie kan worden uitgevoerd door de inspectiedienst van het CCB, door de aangewezen sectorale inspectiedienst of door beide. Het doel van gezamenlijke inspecties of inspecties die aan sectorale inspectiediensten worden gedelegeerd, is het vereenvoudigen en rationaliseren van overheidsmiddelen.

De inspecteurs kunnen op locatie gaan, hun vaststellingen optekenen en verslagen opstellen. Op basis van deze vaststellingen kan een procedure worden opgestart om de entiteit aan te manen een einde te maken aan de inbreuk en, indien nodig, de gepaste administratieve maatregelen te nemen, gaande van een waarschuwing tot een administratieve boete.

4.16. Wat moet ik doen als mijn organisatie na 18 maanden nog niet kan aantonen dat ze aan de eisen voldoet?

Tijdens hun controles zullen de inspectiediensten veel nadruk leggen op de evolutie die een organisatie in de loop der tijd heeft doorgemaakt om haar doel te bereiken. Het is dus van groot belang dat bewijs kan worden geleverd van praktische vooruitgang op weg naar naleving.

Het primaire doel van de CCB is het bereiken van een hoog niveau van cyberbeveiliging in het hele land, in nauwe samenwerking met alle betrokken entiteiten. Er zijn echter situaties waarin sancties nodig kunnen zijn. Daartoe voorziet de wet (titel 4, sectie 2) in een specifieke procedure die de interactie tussen het CCB en de betrokken entiteit vastlegt. Deze procedure omvat met name de verplichting voor het CCB (of een sectorale autoriteit) om de entiteit te informeren over zijn voornemen om een sanctie op te leggen. Het spreekt voor zich dat dit ontwerp van sanctiebeslissing vergezeld moet gaan van een voldoende motivering. De entiteit heeft dan de mogelijkheid om zich te verdedigen.

Als een sanctie toch nodig wordt geacht, moet het CCB rekening houden met een bepaald minimumaantal elementen om een passende en evenredige sanctie te bepalen; bijvoorbeeld de categorie van de entiteit, eerdere overtredingen, de ernst van de overtreding, de duur ervan, schade, nalatigheid, enz.

In elk geval kan de bevoegde inspectiedienst bij niet-naleving passende maatregelen en/of boetes opleggen om ervoor te zorgen dat de organisatie de wet naleeft. Afhankelijk van het effect van deze maatregelen en/of boetes op het gedrag van de organisatie, kunnen verdere maatregelen en/of boetes worden opgelegd totdat naleving is bereikt.

Meer informatie over maatregelen en boetes is te vinden in de secties 4.17 en .

4.17. Zijn administratieve maatregelen en boetes evenredig? Hoe hoog zijn de boetes?

Art. 59 NIS2-wet

Het doel van administratieve maatregelen en boetes is om het niveau van cyberbeveiliging van essentiële en belangrijke entiteiten te verhogen. Op voorwaarde dat de wettelijke procedures worden nageleefd (inclusief het horen van de betrokken entiteit, zie artikel 51-57), kan een administratieve maatregel of boete worden opgelegd, op een proportionele manier, rekening houdend met de ernst van de inbreuken, de houding van de entiteit en eventuele recidive.

De volgende administratieve geldboetes kunnen worden opgelegd:

1. Van 500 tot 125.000 euro voor iedereen die niet voldoet aan de informatieverplichtingen waarnaar wordt verwezen in artikel 12;
2. Van 500 tot 200.000 euro voor een entiteit die een persoon die namens haar handelt nadelige gevolgen berokkent ingevolge de uitvoering, te goeder trouw en binnen het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet;
3. Van €500 tot €200.000 voor iedereen die niet voldoet aan de toezichtverplichtingen;
4. Van 500 tot 7.000.000 euro of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort (afhankelijk van welk bedrag het hoogst is), de belangrijke entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of de rapportageverplichtingen;
5. Van 500 tot 10.000.000 euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort (afhankelijk van welk bedrag het hoogst is), de essentiële entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

4.18. Welke andere administratieve maatregelen kunnen worden genomen?

4.18.1. Basismaatregelen

De volgende administratieve maatregelen kunnen worden opgelegd aan essentiële en belangrijke entiteiten:

Art. 58 NIS2-wet

1. waarschuwingen geven over inbreuken door de betrokken entiteiten op deze wet;
2. bindende aanwijzingen vaststellen of een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze wet te verhelpen;
3. de betrokken entiteiten gelasten een einde te maken aan gedragingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;
4. de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met titel 3 of te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel;
5. de betrokken entiteiten gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;
6. de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;
7. de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;

Wanneer de betrokken entiteit een essentiële entiteit is:

- het CCB kan voor een bepaalde periode een controlefunctionaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor het beheer van cyberbeveiligingsrisico's en inzake het melden van incidenten
- de in punt 2 bedoelde bindende aanwijzingen omvatten ook de maatregelen die nodig zijn om een incident te voorkomen of te verhelpen, alsmede uiterste termijnen voor de uitvoering van dergelijke maatregelen en voor verslaggeving over de uitvoering ervan.

4.18.2. Bijkomende maatregelen

Als de gevraagde maatregelen niet binnen de gestelde termijn worden ondernomen, kunnen de volgende administratieve maatregelen worden opgelegd aan essentiële entiteiten:

Art. 60 NIS2-wet

1. een certificering of vergunning tijdelijk opschorten met betrekking tot alle of een deel van de relevante door de betrokken entiteit verleende diensten of verrichte activiteiten;
2. natuurlijke personen met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijk vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leidinggevende verantwoordelijkheden in die entiteit uit te oefenen.

De in punt 1 bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit die deze handhavingsmaatregelen heeft opgelegd.

5. Andere

5.1. Geeft de NIS2-richtlijn de Europese Commissie een mandaat voor uitvoeringshandelingen? Waar kan ik deze terugvinden?

Art. 21, § 5 & 23, § 11 NIS2-richtlijn

Er is een uitvoeringsverordening van de Commissie goedgekeurd: Uitvoeringsverordening van de Commissie (EU) 2024/2690 van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten.

Deze uitvoeringsverordening is beschikbaar in Eur-Lex.

De NIS2-richtlijn geeft de Europese Commissie de bevoegdheid om in specifieke gevallen een uitvoeringsverordening aan te nemen.

Artikel 21, § 5, lid 1 van de richtlijn betreft de **technische en methodologische vereisten met betrekking tot maatregelen voor het beheer van cyberbeveiligingsrisico's** voor NS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten en aanbieders van vertrouwensdiensten.

Artikel 23, § 11 van de Richtlijn behandelt het **concept 'significant incident'** voor DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten.

De NIS2-richtlijn voorziet ook in de (optionele) mogelijkheid van andere uitvoeringsverordeningen:

- een uitvoeringsverordening tot vaststelling van technische en methodologische vereisten en sectorale vereisten voor andere soorten essentiële en belangrijke entiteiten (art. 21, § 5, lid 2) ;
- een uitvoeringsverordening waarin het soort informatie, het formaat en de procedure voor meldingen en communicatie met betrekking tot het melden van incidenten nader worden gespecificeerd (art. 23, § 11, lid 1) ;
- een uitvoeringsverordening waarin het concept 'significant incident' voor andere soorten essentiële en belangrijke entiteiten nader wordt uitgewerkt (art. 23, § 11, lid 2, in fine);

Op dit moment is er echter nog geen project voor deze uitvoeringsverordeningen.

5.2. Is er een specifieke persoon binnen een organisatie die verantwoordelijk is voor het implementeren van de cyberbeveiligingsmaatregelen?

De NIS2-wet vereist niet dat er een specifieke persoon (zoals een DPO in het kader van de AVG) binnen de organisatie wordt aangesteld die verantwoordelijk is voor de implementatie van de NIS2-vereisten.

5.3. Bestaat er een openbare lijst van alle essentiële en belangrijke entiteiten?

De NIS2-richtlijn vereist dat lidstaten een lijst van alle essentiële en belangrijke entiteiten opstellen en statistische informatie over deze lijst (aantal entiteiten per sector of deelsector) verstrekken aan de samenwerkingsgroep NIS en de Europese Commissie.

Art. 3, § 3 - 6 richtlijn NIS2

Deze lijst is echter niet openbaar beschikbaar.

6. Concordantietabel

FAQ versie 1.0	FAQ versie 2.0
1.1	1.1
	1.2
1.2	1.3
	1.4
1.3	1.5
	1.6
1.4	1.7
	1.8
1.5	1.9
1.6	1.10
1.7	1.11
1.8	1.12
	1.13
1.9	1.14
	1.15
	1.15.1
	1.15.2
	1.15.3
	1.15.4
	1.15.5
	1.16
	1.16.1
	1.16.2
	1.16.3
	1.16.4
	1.16.5
	1.16.6
	1.16.7
1.10	1.17
1.11	1.18
1.12	2.7
1.13	1.19
	1.20
1.14	1.21
1.14.1	1.21.1
	1.21.2
1.14.2	1.21.3
1.14.3	1.21.4
1.14.4	1.21.5
1.14.5	1.21.6
	1.22

	1.22.1
	1.22.2
	1.22.3
	1.22.4
	1.22.5
	1.22.6
	1.22.7
	1.22.8
	1.22.9
	1.22.10
	1.22.11
	1.22.12
2.1	2.1
	2.2
	2.2
2.2	2.4
2.3	2.5
	2.6
	2.7
	2.8
	2.9
3.1	3.1
3.2	3.2
3.3	3.3
3.3.1	3.3.1
	3.3.2
3.3.2	3.3.3
3.3.3	3.3.4
3.3.4	3.3.5
3.3.5	3.3.6
	3.4
3.4	3.5
3.5	3.6
	3.7
	3.8
	3.11
3.6	3.12
3.7	3.13
	3.13.1
	3.13.2
	3.13.3
	3.13.4
	3.13.5
	3.13.6
	3.13.7

	3.13.8
	3.13.9
	3.13.10
3.8	3.14
3.9	3.15
4.1	4.1
4.1.1	4.1.1
4.1.2	4.1.2
4.1.3	4.1.3
4.2	4.2
4.2.1	4.2.1
4.2.2	4.2.2
	4.3
4.3	4.4
	4.5
4.4	4.6
	4.7
4.5	4.8
4.6	4.9
	4.10
4.7	4.11
	4.12
4.8	4.13
4.9	4.14
4.10	4.15
	4.16
4.11	4.17
4.12	4.18
4.12.1	4.18.1
4.12.2	4.18.2
4.13	3.9
4.14	3.10
5.1	5.1
	5.2
	5.3