# Afstemming van de PSI- en NIS-richtlijnen

## I) Context

In het kader van de omzetting van de PSI-richtlijn[1] is de vraag gerezen hoe deze is afgestemd op de NIS-richtlijn[2].

Om mogelijke problemen op te sporen die de omzetting van de PSI-richtlijn zou kunnen veroorzaken, gelet op de NIS-richtlijn, is het belangrijk om enerzijds de respectieve doelstellingen van deze richtlijnen vast te stellen en anderzijds de maatregelen die worden genomen om deze doelstellingen te bereiken en het toepassingsgebied van deze maatregelen.

## II) Wetgevend kader

### 1) Europees recht

#### a) Doel van de richtlijn

- **PSI-richtlijn**

Het doel van de PSI-richtlijn is "*het gebruik van open data te bevorderen en innovatie in producten en diensten te stimuleren*"[3].

- **NIS-richtlijn**

Het doel van de NIS-richtlijn is het vaststellen van maatregelen "*met het oog op het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, teneinde de werking van de interne markt te verbeteren*"[4].

---

[1] Richtlijn nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), PB, L 172/56.
[2] Richtlijn nr. 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, PB, L 194/1.
[3] Richtlijn nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), PB, L 172/56, art. 1, 1.
[4] Richtlijn nr. 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, PB, L 194/1.
[4] Richtlijn nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), PB, L 172/56, art. 1, 1.

## b) Maatregelen en toepassingsgebied

- **PSI-richtlijn**

Om het gebruik van open data aan te moedigen, vereist de PSI-richtlijn dat bepaalde documenten en gegevens worden opengesteld.

Zo moeten bijvoorbeeld documenten "die in het bezit *zijn van **openbare lichamen** van de lidstaten*", documenten "*die in het bezit zijn van [bepaalde] **overheidsondernemingen**"* en "***onderzoeksgegevens***" openstaan voor hergebruik[5].

Volgens artikel 2, 1), van de PSI-richtlijn wordt onder ***"openbare lichamen***" verstaan "*de staat, zijn territoriale lichamen, publiekrechtelijke instellingen, en verenigingen gevormd door een of meer van deze lichamen of een of meer van deze publiekrechtelijke instellingen*".

In artikel 2, 2), van de richtlijn wordt het begrip "***overheidsonderneming***" gedefinieerd als "*elke onderneming die actief is op de in artikel 1, lid 1, onder b)* [6]*, genoemde gebieden en waarop de openbare lichamen direct of indirect een overheersende invloed kunnen uitoefenen uit hoofde van eigendom, financiële deelname of de op de onderneming van toepassing zijnde voorschriften. Er wordt uitgegaan van een overheersende invloed van de openbare lichamen in elk van de volgende gevallen waarin die lichamen, direct of indirect:*

> *a) de meerderheid van het geplaatste kapitaal van de onderneming bezitten;*
> *b) over de meerderheid van de stemrechten verbonden aan de door de onderneming uitgegeven aandelen beschikken;*

---

[5] Richtlijn nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), PB, L 172/56, art. 1, 1.

[6] Krachtens dit artikel moeten de volgende overheidsondernemingen hun gegevens openstellen voor hergebruik:

I) elke overheidsonderneming die activiteiten verricht binnen de in richtlijn 2014/25/EU omschreven domeinen (deze sectoren zijn: Gas en warmte, Elektriciteit, Water, Vervoersdiensten, Havens en luchthavens, Postdiensten, Olie- en gaswinning en exploratie en winning van steenkool en andere vaste brandstoffen);

II) elke overheidsonderneming die optreedt als exploitant van overheidsdiensten overeenkomstig artikel 2 van Verordening (EG) nr. 1370/2007 (dit zijn: elke onderneming of groep van publiekrechtelijke of privaatrechtelijke ondernemingen die openbare personenvervoersdiensten exploiteert of elke overheidsinstantie die openbare personenvervoersdiensten aanbiedt);

III) elke overheidsonderneming die optreedt als luchtvaartmaatschappij die voldoet aan de openbaredienstverplichtingen overeenkomstig artikel 16 van Verordening (EG) nr. 1008/2008 (het gaat om een "een openbaredienstverplichting met betrekking tot geregelde luchtdiensten tussen een luchthaven in de Gemeenschap en een luchthaven die de luchtverbindingen voor een perifeer of ontwikkelingsgebied verzorgt"); of

IV) elke overheidsonderneming die optreedt als communautaire reder die voldoet aan openbaredienstverplichtingen overeenkomstig artikel 4 van Verordening (EEG) nr. 3577/92 (Het gaat om: openbare-dienstcontracten met rederijen die deelnemen aan geregelde diensten van en naar eilanden en tussen eilanden onderling of die hun openbare-dienstverplichtingen opleggen als voorwaarde voor het verrichten van cabotagediensten).

*c) meer dan de helft van de leden van het bestuurs-, het leidinggevend of het toezichthoudend orgaan van de onderneming kunnen aanwijzen".*

Ten slotte *worden* "***onderzoeksgegevens***" gedefinieerd als "*andere documenten in digitale vorm dan wetenschappelijke publicaties, die worden verzameld of geproduceerd tijdens wetenschappelijke onderzoeksactiviteiten en die als bewijs in het onderzoeksproces worden gebruikt, of waarvan binnen de onderzoeksgemeenschap algemeen wordt erkend dat ze noodzakelijk zijn om onderzoeksresultaten te valideren*" [7].

- **NIS-richtlijn**

Zoals we hebben gezien, is het doel van de NIS-richtlijn om "*maatregelen [vast te stellen] met het oog op het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, teneinde de werking van de interne markt te verbeteren*".

Daartoe worden in artikel 1, 2. de verschillende maatregelen opgesomd die door de richtlijn zijn ingevoerd.

In dit artikel wordt bepaald dat de richtlijn: "

*a) de vaststelling van verplichtingen voor alle lidstaten om **een nationale strategie** voor beveiliging van netwerk- en informatiesystemen **vast te stellen**;*

*b) **de instelling van een samenwerkingsgroep** die de strategische samenwerking en informatie-uitwisseling tussen de lidstaten moet ondersteunen en onderling vertrouwen moet scheppen*

*c) de **totstandbrenging** van een netwerk van computer security incident response teams („**CSIRT's-netwerk**") dat mede vertrouwen moet scheppen tussen de lidstaten en snelle en doeltreffende operationele samenwerking moet bevorderen;*

*d) de **vaststelling van beveiligings- en meldingseisen** voor **aanbieders van essentiële diensten** en voor **digitaledienstverleners**;*

*e) de vaststelling van verplichtingen voor de lidstaten om **nationale bevoegde autoriteiten, centrale contactpunten en CSIRT's aan te wijzen**, met taken in verband met de beveiliging van netwerk- en informatiesystemen;*

Deze maatregelen kunnen worden ingedeeld naargelang ze een verplichting voor de lidstaten inhouden, maatregelen zijn die op Europees niveau zijn ingevoerd of maatregelen die zijn opgelegd aan aanbieders van essentiële diensten of digitaledienstverleners.

- aan de lidstaten opgelegde verplichtingen.

Wat de aan de lidstaten opgelegde verplichtingen betreft, voorziet artikel 1, 2., van de richtlijn in de vaststelling van een "*nationale strategie voor beveiliging van netwerk- en informatiesystemen*"

[7] Richtlijn nr. 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (herschikking), PB, L 172/56, artikel 2, 9).

en in de aanwijzing van "*nationale bevoegde autoriteiten*", "*centrale contactpunten*" en "*CSIRT's*". Deze verplichtingen worden nader omschreven in respectievelijk artikel 7, 8 en 9.

Daarnaast zijn de lidstaten ook verantwoordelijk voor het aanwijzen van *aanbieders van essentiële diensten* "*voor elke in bijlage II genoemde sector en deelsector (...) met een vestiging op hun grondgebied*"[8].

- Genomen maatregelen op Europees niveau

De "samenwerkingsgroep" en het "CSIRT-netwerk" zijn organen die op Europees niveau zijn opgericht.

de samenwerkingsgroep bestaat uit *"vertegenwoordigers van de lidstaten, de Commissie en het ENISA*"[9] en het CSIRT-netwerk uit "*vertegenwoordigers van de CSIRT's van de lidstaten en CERT-EU*"[10].

- beveiligings- en meldingsvereisten voor de "*aanbieders van essentiële diensten*" en de "*digitaledienstverleners*".

Het begrip "***aanbieder van essentiële diensten***" wordt in artikel 4, 4), gedefinieerd als elke "*publieke of private entiteit waarvan de soort is vermeld in bijlage II en die voldoet aan de criteria van artikel 5, lid 2*".

In bijlage II bij de NIS-richtlijn worden de "*soorten entiteiten in de zin van artikel 4, punt 4"* genoemd.

Daartoe identificeert ze verschillende activiteitensectoren: "

1. *Energie*
2. *Vervoer*
3. *Bankwezen*
4. *Infrastructuur voor de financiële markt*
5. *Gezondheidszorg*
6. *Levering en distributie van drinkwater*
7. *Digitale infrastructuur*".

[8] Richtlijn nr. 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB, L 194/1, artikel 5, 1.
[9] Richtlijn nr. 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB, L 194/1, art. 11, 2.
[10] Richtlijn nr. 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, PB, L 194/1, art. 12, 2.

Vervolgens worden in de bijlage voor elk van deze sectoren, waar van toepassing, bepaalde subsectoren geïdentificeerd en ten slotte worden de entiteiten *per se* kort gedefinieerd.

Artikel 5, §2, bepaalt dat "*De in artikel 4, punt 4, bedoelde criteria voor de identificatie van aanbieders van essentiële diensten luiden als volgt:*

*a) een entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;*

*b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen, en*

*c) een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst".*

Het begrip "***digitaledienstverleners***" wordt in artikel 4, 6), van de richtlijn gedefinieerd als "elke *rechtspersoon die een digitale dienst aanbiedt*".

De richtlijn maakt een onderscheid tussen "beveiligings- en meldingsvereisten" voor aanbieders van essentiële diensten en die voor digitaledienstverleners[11].

In wezen zijn deze vereisten echter in grote lijnen vergelijkbaar en hebben ze betrekking op de preventie en het beheer van risico's die de veiligheid van de netwerk- en informatiesystemen van de aanbieder of dienstverlener bedreigen en op de melding aan de bevoegde autoriteiten van incidenten die een aanzienlijke invloed hebben gehad op respectievelijk de essentiële dienst of de levering van de digitale dienst.

## 2) Belgisch recht

Tot op heden is alleen de NIS-richtlijn in Belgisch recht omgezet.

Deze richtlijn is omgezet in drie wetten:

- De wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector[12];
- De wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren[13]; en

[11] De beveiligings- en meldingsvereisten voor aanbieders van essentiële diensten worden in artikel 14 gespecificeerd en die voor digitaledienstverleners worden in artikel 16 van de richtlijn gedefinieerd.

[12] Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, *B.S.*, 24 januari 2003.

[13] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *B.S.*, 15 juli 2011.

- De wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid[14].

Om de NIS-richtlijn volledig om te zetten heeft de wetgever de wetten van 17 januari 2003 en 1 juli 2011 gewijzigd in de wet van 7 april 2019.

- **Wet van 17 januari 2003**

De wet van 7 april 2019 wijzigt artikel 14 van de wet van 17 januari 2003 dat de opdrachten van het *"Belgisch Instituut voor Postdiensten en Telecommunicatie"* preciseert (hierna het "BIPT").

Voortaan is, krachtens artikel 14, 3°, een van de opdrachten van het BIPT *"het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan":*

> *(…)*
> *g) de **wet van 1 juli 2011** betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;*
> *h) de **wet van 7 april 2019** tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuren; (…)*

*Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt **het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren.** De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut".*

Zo krijgt het BIPT de rol van **"sectorale overheid"**. Dit begrip wordt niet gedefinieerd door de wet van 17 januari 2003[15].

Op dit punt moet rekening worden gehouden met de wet van 1 juli 2011.

- **Wet van 1 juli 2011**

[14] Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, *B.S.,* 3 mei 2019.
[15] De wet van 7 april 2019 bepaalt in zijn artikel 6, 2°, enkel dat het een "*sectorale overheid"* is, "*aangewezen door de wet of de Koning bij besluit vastgesteld na overleg in de Ministerraad"*.

Vooreerst wijst artikel 3, 3°, van deze wet voor elke sector die hij identificeert een "sectorale overheid" aan. De bevoegdheden van deze overheden worden vervolgens gedetailleerd in de artikelen 5 tot en met 11.

In wezen zijn deze overheden belast met de identificatie van de "***kritieke infrastructuren***", volgens een procedure die wordt bepaald in de bijlage bij de wet[16].

Volgens de wet van 1 juli 2011 wordt een kritieke infrastructuur gedefinieerd als een "*installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken*[17]*."*

De identificatie van de kritieke infrastructuren in de zin van de wet van 2011 is belangrijk voor de identificatie van de aanbieders van essentiële diensten voor de NIS-richtlijn, aangezien artikel 18 van de wet van 7 april 2019 stelt dat *"(…), de sectorale overheid de* ***exploitanten van kritieke infrastructuren*** *aanstelt (…), als* ***aanbieders van essentiële diensten****, wanneer* ***hun sector is opgenomen in bijlage I*** *van deze wet* ***en de verlening van hun essentiële diensten afhankelijk is van netwerk- en informatiesystemen***".

Paragraaf 2 van dit artikel stelt echter dat "***behoudens tegenbewijs, de exploitatie van een kritieke infrastructuur geacht*** *wordt* ***afhankelijk te zijn*** *van netwerk- en informatiesystemen".*

Met andere woorden, wanneer een kritieke infrastructuur actief is in een sector opgenomen in bijlage I van de wet van 7 april 2019 en deze afhankelijk is van netwerk- en informatiesystemen – eigenschap die door de wet wordt vermoed –, dan wordt ze door de sectorale overheid aangesteld als een aanbieder van essentiële diensten.

- **Wet van 7 april 2019**

De wet van 7 april 2019 vormt het grootste deel van de omzetting van de NIS-richtlijn in Belgisch recht door te zorgen voor de omzetting van alle *supra* geïdentificeerde verplichtingen die de lidstaten krachtens de NIS-richtlijn hebben.

[16] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *B.S.* 15 juli 2011, art. 5, §2.
[17] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *B.S.* 15 juli 2011, art. 3, 4°.

Zo bepaalt artikel 7 van de wet van 7 april 2019 ten eerste dat "*de Koning de autoriteit aanwijst die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet".* Het betreft de "**bevoegde nationale autoriteit"** in de zin van artikel 8 van de richtlijn*.*

De Koning heeft deze autoriteit aangewezen door middel van een koninklijk besluit van 12 juli 2019[18]. Het betreft het "CCB", het Centrum voor Cybersecurity België.

Vervolgens behandelt artikel 10 **de nationale strategie voor de beveiliging van netwerk- en informatiesystemen**. Deze strategie moet *"passende strategische en regelgevingsdoelstellingen bepalen om een hoog niveau van beveiliging van netwerk- en informatiesystemen tot stand te brengen en te handhaven"* [19]*.* De bijwerking van deze strategie valt onder de bevoegdheid van het CCB[20].

**De identificatie van de aanbieders van essentiële diensten** wordt geregeld door de artikelen 11 tot en met 19 van de wet.

In wezen bepalen deze artikelen dat de aanbieders van essentiële diensten door de sectorale overheden worden geïdentificeerd in elk van hun sectoren, op basis van bepaalde criteria. Op dit punt herinneren we er eveneens aan dat, krachtens artikel 18 van de wet, de kritieke infrastructuur – in de zin van de wet van 1 juli 2011 – die actief is in een van de sectoren die worden geïdentificeerd in bijlage I van de wet van 7 april 2019, in principe wordt aangewezen als aanbieder van essentiële diensten.

De artikelen 20 tot en met 31 van de wet behandelen de veiligheidsvereisten waaraan de aanbieders van essentiële diensten moeten voldoen en de melding van de incidenten die deze aanbieders in voorkomend geval zouden ondergaan.

Wat de **digitaledienstverleners** betreft, is er geen sprake van een identificatieprocedure *per se*[21]; de identificatie van deze aanbieders moet dus per geval worden uitgevoerd met het oog op de definitie in artikel 6, 21°, van de wet van 7 april 2019, die bepaalt dat een aanbieder van digitale diensten *"een rechtspersoon is die een digitale dienst als bedoeld in bijlage II van deze wet verleent*".

---

[18] Koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren*, B.S.,* 18 juli 2019, art. 3, §1.

[19] Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, B.S., 3 mei 2019, art. 10, §2, 2e lid.

[20] Koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *B.S.,* 18 juli 2019, art. 3, §1.

[21] Artikel 32 van de wet bepaalt enkel dat: "deze titel niet van toepassing is op micro- en kleine ondernemingen zoals gedefinieerd in de aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen".

Bijlage II identificeert 3 sectoren: de sector "*onlinemarktplaats*", de sector van de "*onlinezoekmachines*" en de sector van de "*cloudcomputerdiensten*".

Voor het overige preciseert de wet van 7 april 2018 zoals voor de aanbieders van essentiële diensten, de veiligheidsvereisten waaraan de digitaledienstverleners moeten voldoen en behandelt ze de melding van incidenten die gevolgen hebben voor deze dienstverleners.

Tot slot richt de wet een nationaal **CSIRT**, alsook verschillende sectorale CSIRT's op om de integrale omzetting van de NIS-richtlijn te garanderen. De bepalingen betreffende de – nationale en sectorale – CSIRT's worden gepreciseerd in de artikelen 60 tot en met 64.

## III) Onderlinge afstemming van de PSI-richtlijn en de NIS-wetgeving

### a) Afbakening van het probleem

Vooreerst moet worden opgemerkt dat de PSI-richtlijn slechts één keer verwijst naar de NIS-richtlijn, namelijk in overweging 26, die het volgende stelt: *"In deze richtlijn is geen algemene verplichting opgenomen om toestemming te verlenen voor het hergebruik van documenten van overheidsondernemingen. De betrokken overheidsondernemingen moeten zelf kunnen beslissen of ze al dan niet toestemming verlenen voor hergebruik, tenzij anders vereist door deze richtlijn of door Unie- of nationaal recht. (…)* ***Wanneer toestemming wordt verleend voor het hergebruik van documenten, moet er bijzondere aandacht worden besteed aan gevoelige informatie in verband met*** *(…)* ***essentiële diensten in de zin van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad****".*

Zo blijkt deze overweging dus geen specifieke verplichting in te houden – afgezien van de verplichting om rekening te houden met het al dan niet gevoelige karakter van de informatie – betreffende het openstellen van informatie die in het bezit is van een aanbieder van essentiële diensten.

Bovendien kunnen in het kader van de omzetting van de PSI-richtlijn in Belgisch recht enkel bepaalde maatregelen van de NIS-richtlijn – meer bepaald omgezet door de wet van 7 april 2019 – eventueel voor problemen zorgen.
Van de door de richtlijn ingevoerde maatregelen lijkt bijvoorbeeld de vaststelling van een nationale strategie voor de beveiliging van netwerk- en informatiesystemen immers geen belemmering te vormen voor het openstellen van bepaalde gegevens voor hergebruik, aangezien deze strategie in voorkomend geval op initiatief van het CCB kan evolueren.

Ook de aanwijzing van bevoegde nationale overheden, van een centraal contactpunt of van een CSIRT; lijkt niet van aard om een belemmering te vormen voor deze opstelling van gegevens.

Indien een aanbieder van essentiële diensten of een digitaledienstverlener – in de zin van de nationale en Europese NIS-wetgeving – eveneens de hoedanigheid heeft van een entiteit die de gegevens die ze in haar bezit heeft moet openstellen voor hergebruik – krachtens de PSI-richtlijn –, kunnen de veiligheids- en meldingsvereisten waaraan ze moeten voldoen deze openstelling echter belemmeren.

### b) Betreffende de veiligheids- en meldingsvereisten in het bijzonder

We hebben gezien dat de wet van 7 april 2019 de omzetting in Belgisch recht vormt van het systeem van veiligheidsvereisten waaraan de aanbieders van essentiële diensten en de digitaledienstverleners moeten voldoen.

Artikel 17 van deze wet bevat een belangrijke precisering betreffende de documenten in het bezit van de **aanbieders van essentiële diensten**. Zo stelt dit artikel dat: "*Onverminderd de eventuele toepassing van de wet van 11 december 1998*[22]*, **de bestuursdocumenten betreffende de toepassing van dit hoofdstuk**[23] **als bestuursdocumenten worden beschouwd** (…) **die niet het voorwerp mogen uitmaken van inzage, uitleg of mededeling in afschrift voor het publiek**".*

Volgens de auteurs van het wetsontwerp preciseert dit artikel "*in welke mate de bestuursdocumenten verbonden aan de toepassing van hoofdstuk 1 van Titel 2 ontsnappen aan de regels van de openbaarheid van het bestuur*" [24].

Artikel 1, 2., d), van de PSI-richtlijn stelt echter dat "***deze richtlijn niet van toepassing is op***:
(…)
*d) **documenten,** zoals gevoelige gegevens, **waartoe de toegang is uitgesloten op basis van de toegangsregelingen van de lidstaat**, onder meer wegens:*

> *i) de bescherming van de nationale veiligheid (namelijk staatsveiligheid), defensie of openbare veiligheid;*
> *ii) statistisch geheim;*
> *iii) handelsgeheim (waaronder bedrijfs- of beroepsgeheim); (…)».*

Uit de combinatie van deze twee bepalingen blijkt dus dat **de documenten die in het bezit zijn van aanbieders van essentiële diensten** die hun documenten zouden moeten openstellen in toepassing van de PSI-richtlijn, **niet moeten worden meegedeeld aan het publiek en, *a fortiori*, dus niet het voorwerp kunnen uitmaken van hergebruik.**

---

[22] Het betreft de wet van 11 december 1998 betreffende de classificatie van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *B*.S., 7 mei 1999. Deze wet behandelt onder meer de "classificatie" die bestaat in "de toekenning van een beschermingsniveau door of krachtens de wet (…)".

[23] De titel van het desbetreffende hoofdstuk is: "Identificatie van de aanbieders van essentiële diensten".

[24] Memorie van toelichting van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, B.S., 3 mei 2019, beschikbaar op https://www.lachambre.be/FLWB/PDF/54/3340/54K3340001.pdf, voor het laatst geraadpleegd op 10 juni 2020.

Wat de **digitaledienstverleners** betreft, moet uit het stilzwijgen van de teksten worden afgeleid dat de documenten die zij in hun bezit hebben, voor hergebruik moeten worden opengesteld als deze dienstverleners binnen het toepassingsgebied van de PSI-richtlijn vallen.