Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 51/2022 van 9 maart 2022

Betreft: Advies m.b.t. een voorontwerp van wet *tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging* (artikelen 8 en 21) (CO-A-2022-019)

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna de "Autoriteit"), aanwezig mevrouw Marie-Hélène Descamps en heren Yves-Alexandre de Montjoye en Bart Preneel;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikelen 23 en 26 (hierna "WOG");

Gelet op de 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* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van de heer Vincent Van Quickenborne, Vice-eersteminister en minister van Justitie en Noordzee, (hierna: de aanvrager) ontvangen op 14/01/2022;

brengt op 9 maart 2022 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 14/01/2022 verzocht de aanvrager het advies van de Autoriteit met betrekking tot een voorontwerp van wet *tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging* (hierna: het ontwerp).

2. Het ontwerp heeft tot doel de maritieme beveiliging aan een volledige en grondige herziening te onderwerpen.

Context

3. Binnen het kader van de maritieme beveiliging moet in eerste instantie gewezen worden op het Internationale Verdrag ter beveiliging van de mensenlevens op zee (hierna: SOLAS-Verdrag) en de Internationale Code voor de beveiliging van schepen en havenfaciliteiten (hierna: ISPS-Code). De ISPS-Code bestaat uit drie delen: de preambule, deel A en deel B. Deel A bevat dwingende voorschriften voor alle landen die het SOLAS-Verdrag hebben geratificeerd, terwijl deel B aanbeveling en richtlijnen bevat voor de implementatie van deel A.

4. De Verordening (EG) Nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 *betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten* (hierna: ISPS-Verordening) verplicht de Europese lidstaten om de ISPS-Code (waaronder tevens neen aantal bepalingen van deel B van de ISPS-Code[1]) effectief toe te passen.

5. De ISPS-Code en de ISPS-Verordening zijn echter beperkt tot beveiligingsmaatregelen aan boord van schepen en de havenfaciliteiten. Echter om de maritieme industrieën optimaal te beschermen was de Europese Commissie van oordeel dat ook in de omliggende gebieden de noodzakelijke maatregelen moeten worden genomen om de beveiliging te kunnen garanderen. Het initiatief van de Europese Commissie heeft geleid tot richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 *betreffende het verhogen van de beveiliging van havens* (hierna: Havenbeveiligingsrichtlijn).

6. De ISPS-Verordening en de Havenbeveiligingsrichtlijn werden in België geïmplementeerd door de wet van 5 februari 2007 *betreffende de maritieme beveiliging* en het koninklijk besluit van 21 april 2007 *betreffende de maritieme beveiliging*. De voormelde wet van 5 februari 2007 werd opgeheven en opgenomen in het Belgisch Scheepvaartwetboek.

[1] Zie artikel 3.5. ISPS-Verordening.

7. Zoals evenwel volgt uit de Memorie van toelichting was het na 15 jaar tijd om de bestaande regelgeving te herzien en aan te vullen, rekening houdend met de belangrijkste problemen die naar voren kwamen na een bevraging van de belanghebbenden in de maritieme beveiliging. Daartoe werden de volgende kerndoelstellingen geïdentificeerd:
   - hervorming en modernisering van de structuur van de maritieme beveiliging in België;
   - verhogen van de beveiliging van havens en havenfaciliteiten door middel van nieuwe beveiligingsmaatregelen (waaronder de verwerking van biometrische gegevens) in de strijd tegen georganiseerde misdaad;
   - controle op het naleven van het havenverbod overeenkomstig artikel 4, §3*bis* van de wet van 24 februari 1921 *betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen* (hierna: de Drugswet);
   - creëren van een wettelijk kader voor wat betreft het gebruik van bewakingscamera's in het Belgische gedeelte van de Noordzee.

8. Bij het opstellen van het ontwerp kwamen tevens de volgende elementen naar voren die de nodige aandacht verdienen teneinde te kunnen voorzien in een wettelijk kader:
   - de toepasbaarheid van de wet van 21 maart 2007 *tot regeling van de plaatsing en het gebruik van bewakingscamera's* (hierna: de Camerawet) in het Belgische gedeelte van de Noordzee;
   - de aanbeveling nr. 01/2021 van de Autoriteit *betreffende de verwerking van biometrische gegevens*[2].

II. ONDERZOEK TEN GRONDE

a. <u>Voorafgaande opmerking inzake de rechtsgrond</u>

9. Elke norm die de verwerking van persoonsgegevens regelt (en die van nature een inmenging vormt in het recht op bescherming van persoonsgegevens) moet niet alleen noodzakelijk en evenredig zijn, maar ook voldoen aan de eisen van voorspelbaarheid en nauwkeurigheid, zodat de betrokkenen, over wie gegevens worden verwerkt, een duidelijk beeld krijgen van de verwerking van hun gegevens. Krachtens artikel 6.3 van de AVG, gelezen in samenhang met artikel 22 van de *Grondwet* en artikel 8 van het EVRM, moet dergelijke wettelijke norm de essentiële elementen van de met de overheidsinmenging gepaard gaande verwerkingen beschrijven. Het gaat hierbij minstens om:

[2] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.01-2021-van-1-december-2021.pdf.

- het (de) precieze en concrete doeleinde(n) van de gegevensverwerkingen;
- de aanduiding van de verwerkingsverantwoordelijke.

Voor zover de met de overheidsinmenging gepaard gaande verwerkingen van persoonsgegevens een belangrijke inmenging in de rechten en vrijheden van de betrokkenen vertegenwoordigen, omvat de wettelijke bepaling terzake tevens volgende (aanvullende) essentiële elementen:

- de (categorieën van) verwerkte persoonsgegevens die ter zake dienend en niet overmatig zijn;
- de (categorieën van) betrokkenen wiens persoonsgegevens worden verwerkt;
- de (categorieën van) bestemmelingen van de persoonsgegevens, evenals de omstandigheden waarin en de redenen waarom de gegevens worden verstrekt;
- de maximale bewaartermijn van de geregistreerde persoonsgegevens;
- de eventuele beperking van de verplichtingen en/of rechten vermeld in de artikelen 5, 12 tot 22 en 34 AVG.

10. De ingevolge het ontwerp in te voeren gegevensverwerkingen vertegenwoordigen een belangrijke inmenging in de rechten en vrijheden van de betrokkenen. De verwerkingen hebben immers betrekking op bijzondere categorieën van persoonsgegevens in de zin van de artikelen 9 en 10 AVG, ze vinden plaats voor toezichts- en controledoeleinden en kunnen aanleiding geven tot negatieve gevolgen voor de betrokkenen. Het is dus vereist dat alle hierboven opgesomde essentiële elementen van de verwerking opgenomen zijn in het ontwerp.

11. Hierna volgt een artikelsgewijze bespreking van de bepalingen die betrekking hebben op de verwerking van persoonsgegevens, en deze die noodzakelijk zijn om de gegevensverwerkingscontext te kunnen begrijpen. De artikels, tenzij uitdrukkelijk anderszins aangegeven, hebben steeds betrekking op de ontwerpartikelen, en niet op de artikelen die op heden van kracht zijn in het Belgisch Scheepvaartwetboek.

b. <u>Artikel 8 van het ontwerp</u>

12. Artikel 8 van het ontwerp vervangt hoofdstuk 2 van titel 5 van boek 2 van het Belgisch Scheepvaartwetboek, en voorziet in de tenuitvoerlegging van de ISPS-Verordening en de omzetting van de Havenbeveiligingsrichtlijn.

13. Het ontworpen hoofdstuk 2 van titel 5 van boek 2 van het Belgisch Scheepvaartwetboek heeft tot doel (1°) *het invoeren van maatregelen voor de verbetering van de beveiliging van in de internationale handel en voor binnenlands verkeer gebruikte zeeschepen en bijhorende havenfaciliteiten, tegen het gevaar van ongeoorloofde acties;* (2°) *het verhogen van de beveiliging*

ten aanzien van dreigingen van beveiligingsincidenten door het vaststellen van regels inzake beveiliging; (3°) *het beschermen van de personen werkzaam in een haven of havenfaciliteit, op een bouw- of kunstwerk in de maritieme zones of aan boord van zeeschepen*; (4°) *het vaststellen van de maatregelen om de beveiliging van de zeeschepen en bouw- en kunstwerken, met inbegrip van kabels en pijpleidingen, in de Belgische maritieme zones te waarborgen;* (5°) *het vaststellen van mechanismes voor de naleving van dit hoofdstuk.*

Art. 2.5.2.3 Begrippen

14. Cruciaal binnen de context van het ontwerp is de notie 'ongeoorloofde actie'. Immers, zoals dit blijkt uit de algemene doelstellingen (zie punt 13) zijn de nieuwe beveiligingsmaatregelen, dewelke in belangrijke mate een verwerking van persoonsgegevens tot gevolg hebben, gericht tot de bescherming van zeeschepen en havenfaciliteiten tegen het gevaar van ongeoorloofde acties.

15. Het risico op bepaalde ongeoorloofde acties dient tevens in acht genomen te worden bij de beoordeling van de proportionaliteit van de genomen beveiligingsmaatregelen. Immers, gezien de grote verscheidenheid aan havenfaciliteiten moeten deze elk op hun eigen manier beschermd worden[3].

16. Het punt 15° van bovenstaand artikel definieert een 'ongeoorloofde actie' als volgt: *"elke actie die gezien de aard of context ervan schade kan toebrengen aan zeeschepen in het internationale en binnenlands zeescheepvaartverkeer, aan passagiers of lading, of aan de desbetreffende havens of havenfaciliteiten, met inbegrip van het gebruik van zeeschepen om via havens en havenfaciliteiten verboden voorwerpen of producten in- of uit België te brengen, personen of dieren zonder toelating te laten inschepen of ontschepen, of alle hiermee verband houdende activiteiten."*

17. In de Memorie van toelichting worden de volgende activiteiten concreet aangemerkt als ongeoorloofd: terrorisme, piraterij, spionage, sabotage, drugshandel, handel in namaakgoederen, mensensmokkel, illegale handel in exotische dieren. Hoewel de Autoriteit van oordeel is dat de strijd tegen dergelijke activiteiten een geoorloofd doeleinde constitueert, meent zij desalniettemin dat de huidige verwoording van het artikel een te ruime appreciatiemarge laat. Gezien de aard van de gegevensverwerkingen die desgevallend ingezet kunnen worden in het kader van de beveiliging van schepen of havenfaciliteiten is het aangewezen om minstens de categorieën van

[3] De Memorie van toelichting geeft het volgende voorbeeld: *"Een containerterminal of een fruitterminal met import vanuit Latijns-Amerika moet veel beter beveiligd worden dan een zandterminal waarin enkel uit de Noordzee opgebaggerd zand wordt geleverd. Bepaalde minimumvereisten zullen echter voor iedereen moeten gelden, zoals de fysieke afsluiting en de controle op het intact zijn hiervan en de verplichte toegangscontrole van alle voertuigen en personen die toegang wensen tot een havenfaciliteit."*

ongeoorloofde acties uitdrukkelijk te specifiëren in de wet. De passage "*elke actie die … schade kan toebrengen aan …"* geeft verkeerdelijk de indruk dat de geviseerde actoren, bij het uitvoeren van een beveiligingsbeoordeling en het opstellen van een beveiligingsplan, naar eigen goeddunken kunnen bepalen welke acties binnen het toepassingsgebied van de wet vallen. Dit kan aanleiding geven tot misbruiken en staat haaks op het voornemen om de beveiliging van de Belgische haven(s)(faciliteiten), schepen en de Noordzee zoveel mogelijk te harmoniseren.

18. Voor het overige is de Autoriteit van oordeel dat de gedefinieerde begrippen geen aanleiding geven tot bijzondere opmerkingen met betrekking tot de verwerking van persoonsgegevens.

Artikel 2.5.2.4 Toepassingsgebied

19. Voormeld artikel verduidelijkt in eerste instantie, overeenkomstig de bepalingen van de ISPS-Verordening, welke reeksen van zeeschepen buiten het toepassingsgebied van het ontwerp vallen.

20. Vervolgens bepaalt paragraaf 2 de territoriale toepassing binnen het Belgische grondgebied. Daartoe wordt gespecifieerd dat overal waar zeeschepen een interactie uitvoeren met de landszijde aangemerkt wordt als een 'havenfaciliteit'.

21. De overige paragrafen hebben respectievelijk betrekking op de bouw- en kunstwerken en kabels of pijpleidingen in de Belgische maritieme zones, militaire excepties en het verbod om zeeschepen te ontvangen indien er in de haven of de havenfaciliteit geen geldig beveiligingsplan voorhanden is.

22. De Autoriteit neemt er akte van.

Artikelen 2.5.2.5 – 2.5.2.14 (Afdeling 2 - Autoriteiten)

23. De voormelde artikelen handelen over de samenstelling, de werking en het takenpakket van respectievelijk de Nationale Autoriteit voor Maritieme beveiliging (hierna: NAMB) en de Lokale Comités voor Maritieme Beveiliging[4] (hierna: LCMB).

[4] Met als voorzitter de havenbeveiligingsfunctionaris bedoeld in artikel 9 van de Havenbeveiligingsrichtlijn (PSO – *Port Security Officer*).

Artikelen 2.5.2.15 – 2.5.2.46 (Afdeling 3 – Havenbeveiliging en Afdeling 4 – Beveiliging van havenfaciliteiten)

24. De afdelingen 3 en 4 bevatten de regelgeving met betrekking tot het uitvoeren van een beveiligingsbeoordeling en het opstellen van een beveiligingsplan voor de havens en de havenfaciliteiten.

25. De beveiligingsbeoordeling vormt de basis voor de verdere werkzaamheden betreffende het beveiligingsplan en de implementatie ervan. Met name voor wat betreft de havenbeveiligingsbeoordeling moet er rekening worden gehouden met de bijzonderheden van de verschillende delen van de haven(faciliteiten) alsmede met de naburige gebieden indien deze van invloed zijn op de beveiliging in de haven. Daartoe moeten minstens de volgende elementen worden vastgesteld[5]:

> *"1° vaststelling en evaluatie van belangrijke bedrijfsmiddelen en infrastructuren die dienen te worden beschermd;*
>
> *2° vaststelling van* ***de risico's op ongeoorloofde acties****;*
>
> *3° vaststelling van mogelijke dreigingen voor de bedrijfsmiddelen en infrastructuren en de waarschijnlijkheid dat deze zich voordoen, met het oog op de vaststelling en prioritering van beveiligingsmaatregelen;*
>
> *4° vaststelling, selectie en prioritering van maatregelen en procedurele wijzigingen met het oog op het verminderen van de kwetsbaarheid op het vlak van beveiliging en hun effectiviteitsniveau;*
>
> *5° vaststelling van zwakke plekken, met inbegrip van menselijke factoren, in de infrastructuur, beleidsmaatregelen en procedures;*
>
> *6° risicoanalyse van die onderdelen die vatbaar zijn voor spionage, terrorisme en sabotage ten gevolge van buitenlandse invloeden door middel van publieke of private samenwerking."*

26. Na goedkeuring van de beveiligingsbeoordeling door het NAMB[6] wordt een beveiligingsplan opgesteld dat concreet de beveiligingsmaatregelen (waaronder de geviseerde verwerkingen van persoonsgegevens) omschrijft[7] (dat tevens ter goedkeuring moet worden voorgelegd aan het NAMB). Hieruit volgt dat het NAMB de finale verantwoordelijkheid draagt om toe te zien op de proportionaliteit van de voorgestelde maatregelen[8]. In dit kader wijst de Autoriteit nogmaals op de noodzaak om de notie (risico's op) ongeoorloofde acties verder te concretiseren in het ontwerp

---

[5] Artikel 2.5.2.15, zie bovendien de toelichting bij dit artikel in de Memorie van toelichting waar de verschillende in acht te nemen beveiligingsaspecten in detail worden besproken.

[6] Zie de artikelen 2.5.2.16, 2.5.2.31 en 2.5.2.35.

[7] Zie met betrekking tot de beveiligingsaspecten van het beveiligingsplan de toelichting bij artikel 2.5.2.34 in de Memorie van toelichting.

[8] In dit kader kan tevens gewezen worden op de artikelen 2.5.2.6, §2, 2° (*"De NAMB is bevoegd voor de beveiligingsaangelegenheden in havens en havenfaciliteiten"*); 2.5.2.6, §3 en 2.5.2.22.

(punt 17). De constateringen daaromtrent spelen immers een belangrijke rol bij de vaststelling van passende beveiligingsmaatregelen.

27. Tot slot wil de Autoriteit in dit kader nog wijzen op de verplichting in hoofde van de beveiligingsbeambte van een havenfaciliteit (hierna: PFSO – *Port Facility Security Officer*) – die instaat voor het uitvoeren van een beveiligingsbeoordeling van de havenfaciliteit en voor het opstellen van een beveiligingsplan – om te voldoen aan de vormingsvereisten overeenkomstig artikel 2.5.2.39. Daartoe dient de PFSO een examen af te leggen bij een erkende beveiligingsorganisatie of opleidingsinstantie[9] overeenkomstig de modaliteiten die de Koning bepaalt. De organisatie en afwikkeling van dergelijke examens impliceren een verwerking van persoonsgegevens van de kandidaten. Hoewel deze verwerking niet noodzakelijkerwijze een belangrijke inmenging in de rechten en vrijheden van de betrokkenen met zich meebrengt, onderstreept de Autoriteit de noodzaak om de essentiële elementen ervan vast te stellen in het koninklijk besluit dat uitvoering beoogt te geven aan het voormelde artikel[10].

28. Eenzelfde opmerking gaat voor wat betreft de onderrichtingen door de NAMB zoals bedoeld in de artikelen 2.5.2.44 en 2.5.2.66 in zover deze bekrachtigd worden door de Koning overeenkomstig respectievelijk de artikelen 2.5.2.45 en 2.5.2.67 en de vorming van de beveiligingsbeambte van de reder (hierna: CSO – *Company Security Officer*) en van het schip (hierna: SSO – *Ship Security Officer*) overeenkomstig de artikelen 2.5.2.61 en 2.5.2.62.

Artikelen 2.5.2.77 – 2.5.2.81 (Afdeling 9 – ISPS-platform)

29. De bovenstaande artikelen regelen de elektronische informatie-uitwisseling tussen alle actoren betrokken bij de maritieme beveiliging voor de uitvoering van het ontworpen hoofdstuk 2 van titel 5 van boek 2 van het Belgisch Scheepvaartwetboek en zijn uitvoeringsbesluiten en de opslag van de informatie.

30. Op heden wordt gebruik gemaakt van een combinatie van verschillende communicatiemethoden om de informatie-uitwisseling te behandelen tussen de verschillende actoren betreffende gemotiveerde adviezen, goedkeuringen, incidentenmeldingen, … In de Memorie van toelichting wordt verduidelijkt dat dit amalgaan aan communicatiemethoden niet voldoet aan de vereisten opgelegd door de ISPS-Verordening en de Havenbeveiligingsrichtlijn om de beveiligingsinformatie op een beveiligde en uniforme manier te behandelen.

---

[9] Zie afdeling 8 – Erkende beveiligingsorganisaties en opleidingsinstanties (de artikelen 2.5.2.69 – 2.5.2.76).

[10] Met betrekking tot de organisatie van wettelijk voorgeschreven bekwaamheidsproeven of examens verwijst de Autoriteit naar haar advies nr. 86/2021. Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-86-2021.pdf.

31. De NAMB staat in voor het beheer van het ISPS-platform en dient actief bij te dragen tot de doeltreffendheid van de veilige werking van het platform. Volledigheidshalve verduidelijkt de Memorie van toelichting dat het platform ontwikkeld zal worden met inachtneming van de bepalingen van de wet van 7 april 2019 *tot vaststelling van een kader voor de beveiliging van netwerk- en informaticasystemen van algemeen belang voor de openbare veiligheid* (NIS-wet). De Autoriteit neemt er akte van.

32. Artikel 2.5.2.78. bepaalt de doelstellingen van het ISPS-platform:

> *"1° de opslag, opvolging en goedkeuring van alle in dit hoofdstuk vermelde beveiligingsbeoordelingen;*
>
> *2° de opslag, opvolging en goedkeuring van alle in dit hoofdstuk vermelde beveiligingsplannen;*
>
> *3° het melden, opslaan en opvolgen van* ***beveiligingsincidenten***[11]*;*
>
> *4° het melden, opslaan en opvolgen van* ***oefeningen****;*
>
> *5°* ***het uitwisselen van informatie tussen de betrokken actoren****;*
>
> *6° het ingeven, opslaan en opvolgen van inspectierapporten door de verschillende diensten;*
>
> *(…)*
>
> *12° het automatiseren van de verschaffing van de beveiligingsinformatie door vreemde schepen;*
>
> *13°* ***de opslag van de gegevens van de toegangscontrole****;*
>
> *14°* ***het controleren van het naleven van het verbod bedoeld in artikel 4, § 3bis, van de wet van 24 februari 1921*** *betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en*

[11] Naar aanleiding van een verzoek om bijkomende informatie werd door de aanvrager de volgende toelichting verschaft inzake de notie 'beveiligingsincidenten': "*Een definitie van het beveiligingsincident is te vinden in de Voorschrift 1, punt 1, onder 13° van de Hoofdstuk XI-2 van het Internationaal Verdrag voor de beveiliging van mensenlevens op zee (SOLAS). Dit werd overgenomen in de Bijlage I van de Verordening 725/2004 (ISPS-Verordening). De definitie daar is:*

"13. Veiligheidsincident: iedere verdacht handeling of omstandigheid die bedreigend is voor de veiligheid van het schip, met inbegrip van de veiligheid van een booreiland, een hogesnelheidsvaartuig, een havenfaciliteit, een schip/haven raakvlak of een schip-tot-schip-activiteit".

In het voorliggende wetontwerp betreffende maritieme beveiliging werd er echter expliciet voor gekozen om het woord veiligheid waar mogelijk te vervangen door het woord beveiliging. Dit om duidelijk te maken dat specifieke regelingen die in het voorliggende ontwerp worden geregeld niet kunnen worden ingeroepen om de veiligheid (bv voor het voorkomen van arbeidsongevallen) te verzekeren, maar dat de finaliteit steeds moet gekoppeld zijn aan de beveiliging van het schip, de havenfaciliteit of de aanwezige personen. (…)

Artikel 15.11 uit deel B van de ISPS-Code bepaalt dat alle mogelijke bedreigingen in acht moeten worden genomen en geeft een niet-limitatieve lijst van beveiligingsincidenten.

(…)

Deze meldingen omvatten dus alle informatie die noodzakelijk is voor het beoordelen van het beveiligingsincident. ***Dit betreft de feiten maar bevat geen persoonsgegevens van verdachten****. De persoonsgegevens zullen evenwel opgenomen worden in de proces-verbalen die door de bevoegde diensten worden opgesteld naar aanleiding van het beveiligingsincident indien de persoon verdacht wordt van het plegen van een misdrijf. Immers zal ook niet elk beveiligingsincident een misdrijf opleveren. Zo zal een hekwerk dat beschadigd geraakt door een ongeval of een windstoot een beveiligingsincident zijn, maar geen misdrijf. De gegevens van de melder (in zo goed al alle gevallen zal dit de PFSO, zijn/haar adjunct, of de bewakingsagent van de erkende beveiligingsorganisatie zijn) zullen uiteraard wel worden meegedeeld zodat contact kan worden opgenomen voor de verdere evaluatie die vereist is."*

antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen en artikel 4.1.2.48 van het Belgisch Scheepvaartwetboek;

*15° **het controleren van de naleving van het verbod dat personen die krachtens hoofdstuk X van de wet van 20 juli 1990** betreffende de voorlopige hechtenis de voorwaarde om zich niet in een haven of havenfaciliteit te begeven opgelegd hebben gekregen;*

*16° het bijhouden van **de veiligheidsmachtigingen** en aanvragen vereist door dit hoofdstuk;*

*17° **het bijhouden van de lijst van leden van de NAMB, LCMB, Cel Maritieme beveiliging, PFSO en CSO.**"*

33. Hoewel deze opsomming van doelstellingen in zekere zin toelaat een beeld te vormen van de in het ISPS-platform op te nemen gegevens, is het geenszins duidelijk welke actoren concreet instaan voor de verwezenlijking van welke doeleinden, noch tot welke gegevens deze actoren desgevallend toegang hebben. Het lijkt immers moeilijk verantwoordbaar dat elke PSO, PFSO of CSO zonder meer toegang heeft tot de gegevens van de toegangscontrole van alle havenfaciliteiten, alle beveiligingsincidenten of oefeningen, tot alle gegevens met betrekking tot de controle op het havenverbod, de veiligheidsmachtigingen van bepaalde personen….

34. Dit geldt des te meer daar het niet geheel duidelijk is op welke wijze artikel 2.5.2.89 – inzake de toegang tot de persoonsgegevens bedoeld in artikel 2.5.2.**88**[12] voor de doeleinden bedoeld in artikel 2.5.2.**86**[13] – zich verhoudt tot de toegang tot het ISPS-platform. Immers, zoals dit redelijkerwijze lijkt te volgen uit de doelstellingen van het ISPS-platform, zullen, in tegenstelling tot wat volgt uit artikel 2.5.2.89., ook andere actoren dan de NAMB, de LCMB's, de Cel maritieme Beveiliging, het openbaar ministerie, de inlichtingendiensten en de inspectiediensten bedoeld in artikel 4.2.4.4 toegang hebben tot (persoons)gegevens op het ISPS-platform.

35. Als dusdanig vraagt de Autoriteit om in het ontwerp te **specifiëren welke actoren voor welke doelstellingen het ISPS-platform kunnen raadplegen**. Voor wat betreft de gegevens inzake de beveiligingsbeoordelingen en -plannen, beveiligingsincidenten, oefeningen, toegangscontroles, het havenverbod en de personen bedoeld in punt 17° van artikel 2.5.2.78. kan er bijvoorbeeld gewerkt worden aan de hand van gepartitioneerde omgevingen per havenfaciliteit. Op die manier kan de toegang tot de gegevens trapsgewijs georganiseerd worden: de NAMB – als verantwoordelijke voor het beheer van het platform – heeft zicht op alle gegevens; de LCMB's

[12] Ten tijde van het schrijven van dit advies verwijst artikel 2.5.2.89. verkeerdelijk naar artikel 2.5.2.84.

[13] Ten tijde van het schrijven van dit advies verwijst artikel 2.5.2.89. verkeerdelijk naar artikel 2.5.2.82.

hebben toegang tot de gegevens met betrekking tot de havens die onder hun bevoegdheid vallen; de PFSO heeft toegang tot de gegevens met betrekking tot zijn havenfaciliteit, …

36. Artikel 2.5.2.81 vereist dat om toegang te krijgen tot een havenfaciliteit aan de ingang gecontroleerd moet worden of de persoon die toegang wenst te krijgen is opgenomen in het ISPS-platform als een persoon voor wie een verbod overeenkomstig artikel 4, § 3*bis*, van de Drugswet of artikel 4.1.2.48 van het Belgisch Scheepvaartwetboek werd opgelegd of aan wie krachtens hoofdstuk X van de wet van 20 juli 1990 *betreffende de voorlopige hechtenis* de voorwaarde om zich niet in een haven of havenfaciliteit te begeven werd opgelegd.

37. Een dergelijk 'havenverbod' is een autonome straf waarbij het tijdelijk verboden is om zich in één of meerdere havens te begeven en veronderstelt logischerwijze een effectieve controle op zijn naleving. De Autoriteit neemt er akte van dat de persoonsgegevens die verwerkt worden in het kader van deze controle (zie ter zake ook de bespreking van de artikelen 2.5.2.86 tot 2.5.2.95) gecentraliseerd worden in het ISPS-platform. Het geniet immers de voorkeur dat de (gerechtelijke) autoriteiten die een dergelijke straf hebben opgelegd deze informatie slechts eenmalig moeten doorgeven aan het gecentraliseerd platform; eerder dan elke geviseerde havenfaciliteit of haven afzonderlijk te moeten contacteren. Dit komt de informatiebeveiliging ten goede. De Autoriteit benadrukt evenwel, rekening houdend met het feit dat een havenverbod opgelegd kan worden voor één of meerdere havens of havenfaciliteiten, dat deze gegevens enkel toegankelijk mogen zijn voor de actoren die instaan voor de toegangscontrole van de geviseerde haven(s) of havenfaciliteiten[14] (zie ook punt 35). Bovendien is de Autoriteit van oordeel dat het ISPS-platform tot doel heeft de nuttige gegevens met betrekking tot het havenverbod **op te slaan**, met het oog op de controle van de naleving ervan. De controle *an sich*, zoals dit op heden lijkt te volgen uit de voormelde bepalingen, is geen echter doelstelling van het ISPS-platform. De Autoriteit vraagt om de punten 14° en 15° nuttig aan te passen in die zin.

38. Concluderend is de Autoriteit van oordeel dat, rekening houdend met de spilfunctie van het platform binnen de globale beveiligingscontext, de regelgeving inzake het ISPS-platform beter kan en moet afgestemd worden op de bepalingen betreffende de verwerking van persoonsgegevens (waar, op een enkele uitzondering na, het platform nergens ter sprake komt). Zonder afbreuk te doen aan de voordelen van een gecentraliseerd platform voor gegevensuitwisseling, is het op heden niet steeds duidelijk welke van de naar voor geschoven doelstellingen aanleiding kunnen geven tot een verwerking van (welke) persoonsgegevens en door welke actoren. Dit is niet verenigbaar met artikel 6.3 AVG, gelezen in het licht van overweging 41, en artikel 22 *Grondwet.*

[14] In die zin bepaalt de Memorie van toelichting het volgende: *"Doordat het havenverbod voor één of meerdere havens en havenfaciliteiten kan worden opgelegd, moeten deze gegevens zeer correct worden gecontroleerd en ingegeven worden langs overheidszijde. Een persoon die een verbod heeft gekregen voor haven A moet immers toegang kunnen krijgen in haven B, waarbij er niet de minste indicatie mag zijn dat de persoon veroordeeld werd tot een havenverbod."*

Artikelen 2.5.2.82 – 2.5.2.83 (Camerabeelden)

39. Artikel 2.5.2.82 bepaalt dat bewakingscamera's die geïnstalleerd worden door de exploitanten van havens of havenfaciliteiten moeten voldoen aan de bepalingen van de Camerawet.

40. Artikel 3 van de Camerawet bepaalt dat de plaatsing en het gebruik van (private) bewakingscamera's enkel tot doel kan hebben:

    - *"1° misdrijven tegen personen of goederen te voorkomen, vast te stellen of op te sporen;*
    - *2° overlast in de zin van artikel 135 van de nieuwe gemeentewet te voorkomen, vast te stellen of op te sporen, de naleving van gemeentelijke reglementen te controleren of de openbare orde te handhaven."*

    Artikel 9 van dezelfde wet bepaalt de modaliteiten van de verwerking van de beelden van dergelijke bewakingscamera's.

41. Aangezien het ontwerp geen bijzonderheden specifieert met betrekking tot de plaatsing van bewakingscamera's zijn de bepalingen van de Camerawet onverkort van toepassing. De Autoriteit neemt er akte van.

42. Artikel 2.5.2.83, §1 bepaalt dat "*Het gebruik van* ***intelligente camera's*** *met het oog op de automatische nummerplaatherkenning door de exploitanten van havens en havenfaciliteiten is toegelaten."* Bijkomend, in afwijking van artikel 8/1 van de Camerawet is het gebruik van dergelijke intelligente bewakingscamera's tevens toegelaten met het oog op **de automatische herkenning van vaartuigen.**

43. Naar aanleiding van een verzoek om bijkomende informatie specifieert de aanvrager dat de intelligente camera's (ook aangeduid als ANPR-camera's) die geplaatst kunnen worden door de exploitanten van de haven, enkel dienen tot de registratie van nummerplaten overeenkomstig de regels die daarop van toepassing zijn. Artikel 8/1 van de Camerawet bepaalt in die zin: "*Het gebruik van intelligente bewakingscamera's gekoppeld aan registers of bestanden van persoonsgegevens is enkel toegestaan met het oog op de automatische nummerplaatherkenning,* ***op voorwaarde dat de verwerkingsverantwoordelijke deze registers of bestanden verwerkt met inachtneming van de regelgeving met betrekking tot de bescherming van de persoonlijke levenssfeer****."* Dit laat onverlet de overige verplichtingen die op de verwerkingsverantwoordelijke rusten overeenkomstig de Camerawet. Ter zake wijst de Autoriteit er evenwel op dat elke machtiging om intelligente camera's aan te wenden voor dit doeleinde

weinig zinvol lijkt in zoverre de betrokken actoren geen toegang hebben tot de nummerplaatgegevens in het repertorium van de voertuigen dat wordt bijgehouden door het Directoraat-generaal Wegvervoer en Verkeersveiligheid van de FOD Mobiliteit en Vervoer[15]. Het is aldus aan de verwerkingsverantwoordelijken om na te gaan of zij toegang kunnen hebben tot deze gegevens overeenkomstig de relevante regelgeving[16].

44. Bovendien herinnert de Autoriteit aan de verplichting voor de verwerkingsverantwoordelijke om overeenkomstig artikel 35 AVG een gegevensbeschermingseffectbeoordeling uit te voeren wanneer hij voorziet in een verwerking van persoonsgegevens, die gelet op de aard, de omvang, de context en de doeleinden daarvan een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De plaatsing en het gebruik van ANPR-camera's betreft immers een gegevensverzameling op grote schaal door middel van nieuwe technologieën teneinde de locatie of verplaatsing van natuurlijke personen te analyseren[17]. Met betrekking tot de modaliteiten van het uitvoeren van een gegevensbeschermingseffectbeoordeling verwijst de Autoriteit naar de aanbeveling nr. 01/2018[18] van haar rechtsvoorganger, de Commissie voor de bescherming van de persoonlijke levenssfeer, en de handleiding GEB van de Autoriteit[19]. Naar analogie met de gegevensbeschermingseffectbeoordeling die moet worden uitgevoerd in het kader van de verwerking van biometrische gegevens verdient het aanbeveling dat de gegevensbeschermingseffectbeoordeling voor de plaatsing van (intelligente) bewakingscamera's tevens wordt opgenomen in de beveiligingsbeoordeling van de haven(faciliteiten) (zie punt 53).

45. Inzake de automatische herkenning van vaartuigen verduidelijkt de aanvrager vervolgens dat in de havens de verplichting geldt voor alle vaartuigen die daar varen (uitgezonderd pleziervaartuigen) om te beschikken over een zogenaamde AIS-transponder (`*automatic identification system*'). Dit systeem is gelinkt aan het vaartuig en geeft een identificatie van zijn inschrijvingsnummer en van zijn MMSI-nummer (*Maritime Mobile Service Identification*) (de zendvergunning die in België wordt toegekend door het BIPT[20]). De automatische herkenning voor scheepvaart houdt dus in dat indien een schip wordt gedetecteerd in de haven, via de

---

[15] Zie de opmerking in punt 26 van het advies nr. 53/2017 van de Commissie voor de bescherming van de persoonlijke levenssfeer, rechtsvoorganger van de Autoriteit (te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-53-2017.pdf) en de artikelen 6 en 7 van het koninklijk besluit van 20 juli 2001 *betreffende de inschrijving van voertuigen*.

[16] Ter zake verwijst de Autoriteit naar de wet van 19 mei 2010 *houdende oprichting van de Kruispuntbank van de voertuigen* en het koninklijk besluit van 20 juli 2001 *betreffende de inschrijving van voertuigen*.

[17] Overeenkomstig punt 6.4) van de beslissing nr. 01/2019 van het Algemeen secretariaat van de Autoriteit is het uitvoeren van een gegevensbeschermingseffectbeoordeling verplicht voor dergelijke verwerkingen. Deze beslissing, die een uitvoering betreft van artikel 35.4 AVG, is te raadplegen via de volgende link: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf.

[18] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2018.pdf.

[19] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-gegevensbeschermingseffectbeoordeling.pdf.

[20] Zie bijvoorbeeld: https://www.vesselfinder.com.

AIS-connectie de gegevens met betrekking tot de eigenaar of de exploitant van dat schip kunnen worden opgevraagd bij de bevoegde Belgische diensten indien het een Belgisch schip betreft, bij de buitenlandse diensten voor vreemde schepen, of bij hiertoe erkende organisaties (bijvoorbeeld Lloyds) die de data van alle zeeschepen bijhouden. Hoewel deze AIS-connectie plaatsvindt aan de hand van radiosignalen volgt het uit de Memorie van toelichting dat het belangrijk is dat de AIS-signalen worden gekoppeld aan camerabeelden zodanig dat ook de schepen zonder een AIS-transponder kunnen worden gedetecteerd.

46. Aangezien de AIS-connectie en de camerabeelden evenwel onderscheiden systemen zijn, is de Autoriteit van oordeel dat de noodzaak om gebruik te maken van intelligente camera's in de zin van artikel 2, 4°/3, van de Camerawet – te weten een *"bewakingscamera die ook onderdelen en software bevat, die al dan niet gekoppeld aan registers of bestanden, de verzamelde beelden al dan niet autonoom kunnen verwerken*" – voor de automatische herkenning van vaartuigen onvoldoende wordt aangetoond. Immers, indien een vaartuig, in strijd met de op dat schip van toepassing zijnde regelgeving, niet beschikt over een AIS-transponder kan het volstaan dat dit vaartuig wordt gefilmd door middel van 'gewone' bewakingscamera's.

47. Artikel 2.5.2.83, §2, bepaalt: *"Het gebruik van intelligente camera's overeenkomstig paragraaf 1 is toegelaten om de naleving van de ISPS-verordening, de ISPS-Code en dit hoofdstuk en zijn uitvoeringsbesluiten te controleren, evenals het voorkomen van ongeoorloofde acties en het garanderen van de maritieme beveiliging."*

48. Rekening houdend met de omvang van de voormelde regelgevingen en de aard van de verwerkingen aan de hand van intelligente camera's (zie punt 44) is de Autoriteit van oordeel dat deze paragraaf een (te) ruime marge laat voor subjectieve invulling. In zover het gebruik van intelligente camera's noodzakelijk is om de naleving van bepaalde verplichtingen te controleren moet dit uitdrukkelijk blijken uit de wet.

Artikel 2.5.2.84 (Gebruik biometrische gegevens)

49. In de Memorie van toelichting wordt aangehaald dat verschillende havenbedrijven momenteel reeds biometrische gegevens verwerken om te controleren of een persoon toegang kan krijgen tot een bepaalde havenfaciliteit of elektronisch netwerk. De aanbeveling nr. 01/2021 van de Autoriteit *betreffende de verwerking van biometrische gegevens* onderstreept dat sinds de inwerkingtreding van de AVG de nodige rechtsgrond hiervoor ontbreekt in de Belgische regelgeving. De stellers van het ontwerp beweren in dat kader evenwel verkeerdelijk dat de Autoriteit een termijn van 1 jaar heeft toegekend aan deze bedrijven om ofwel het gebruik van de biometrische gegevens uit te faseren ofwel om de wetgever aan te sporen te voorzien in een

juridisch kader. Niet alleen is een dergelijke termijn onverenigbaar met de directe werking van de AVG binnen de Belgische rechtsorde, er dient tevens te worden vastgesteld dat de AVG ondertussen reeds 4 jaar van toepassing is. Elke verwerking van biometrische gegevens die plaatsvindt zonder geldige rechtsgrond geeft aanleiding tot een schending van de AVG. De betrokken passage moet zonder meer geschrapt worden uit de Memorie van toelichting.

50. Zoals dit uitvoerig wordt toegelicht in de aanbeveling nr. 01/2021[21] moet de Belgische wetgever, in zover zij het gebruik van biometrische gegevens voor bepaalde doeleinden op grond van artikel 9.2. g) AVG wil toestaan, de modaliteiten van deze verwerking expliciet bij wet regelen.

51. Artikel 2.5.2.84 onderscheidt drie doeleinden voor de verwerking van biometrische gegevens in havens of havenfaciliteiten:

- in eerste instantie kunnen de beveiligingsplannen – **op basis van concrete elementen in de beveiligingsbeoordelingen die de noodzaak daarvoor aantonen**[22] – voorzien dat de toegang tot een havenfaciliteit afhankelijk wordt gemaakt van verificatie van biometrische gegevens van alle of bepaalde categorieën van bezoekers[23]. De Memorie van toelichting bepaalt dat het gebruik van biometrische gegevens absoluut noodzakelijk is om een correcte toegangscontrole te kunnen uitvoeren. Immers, volgens 'recente informatie' wordt er op de zwarte markt tot 7.500 euro betaald voor een badge waarmee toegang tot een havenfaciliteit kan worden bekomen. Zodra deze badge echter gekoppeld wordt aan biometrische gegevens zal het doorgeven van deze badge niet zonder meer mogelijk zijn;
- ten tweede kan er worden voorzien dat ook de digitale toegang tot bepaalde modules van de netwerk- en informaticasystemen van de haven(faciliteiten) moet gebeuren aan de hand van biometrische systemen[24];
- ten derde kunnen biometrische gegevens worden gebruikt in het kader van de ladingbehandeling (en meer bepaald voor de toegang tot een *straddle carrier* of containerlift

[21] Zie onderafdeling 1.3.2 *Zwaarwegend algemeen belang* van de aanbeveling nr. 01/2021, blz. 25 – 28.

[22] Hoewel dit afgeleid zou kunnen worden uit de bepalingen met betrekking tot de beveiligingsbeoordelingen en -plannen en de Memorie van toelichting lijkt het aangewezen om een verduidelijking in die zin uitdrukkelijk op te nemen in het voormelde artikel.

[23] Voor de toepassing van deze regelgeving bepaalt artikel 2.5.2.84, §3 dat onder 'bezoeker' wordt verstaan *"iedereen, met inbegrip van bestuurders en personeelsleden, die toegang wenst tot de havenfaciliteit of gedeelten van de havenfaciliteit met uitzondering van de passagiers van zeeschepen die inschepen of ontschepen op een havenfaciliteit voor het vervoer van passagiers, en voor bemanningsleden van zeeschepen."*

[24] Uittreksel uit de Memorie van toelichting: *"Een personeelslid dat toegang heeft tot de juiste data kan er bijvoorbeeld voor zorgen dat containers op een bepaalde plaats worden gezet. Door het lekken van de pincodes waarmee een bepaalde lading kan worden opgepikt door de externe transporteur, kan deze lading opnieuw op vrij eenvoudige wijze uit de havenfaciliteit worden gehaald. Een adequate bestrijding van de georganiseerde criminaliteit vereist dan ook dat kan worden nagegaan wie toegang heeft gekregen tot bepaalde informatie en deze voor oneigenlijke doeleinden heeft misbruikt.*

Ook in deze is de uitzonderingsgrond van artikel 9.2, g) van de AVG, namelijk het zwaarwegend algemeen belang, de basis waarop de verwerking van de biometrische gegevens gerechtvaardigd is. Deze uitzondering houdt uiteraard niet in dat de toegang tot het ganse netwerk- en informatiesysteem van een havenfaciliteit onderworpen kan zijn aan het verifiëren van de biometrische gegevens. Enkel die modules die gevoelig zijn voor misbruik kunnen aan deze verplichting worden onderworpen."

die gebruikt wordt om schepen af te laden en, desgevallend om verdachte ladingen af te zonderen voor inspectie[25]).

52. De Autoriteit benadrukt dat het opsommen van de in aanmerking komende doelstellingen geen vrijgeleide is voor de verwerking van biometrische gegevens en dat zij de verwerkingsverantwoordelijke geenszins ontslaat van zijn verplichting om de noodzaak en de evenredigheid van de gegevensverwerking te onderbouwen. Zoals reeds werd toegelicht moet voor elke havenfaciliteit een beveiligingsbeoordeling worden uitgevoerd waarin, onder meer, de risico's op ongeoorloofde acties worden vastgesteld. Concrete elementen (type lading, herkomst van het vaartuig, infrastructuur van de faciliteit, …) zullen in acht moeten worden genomen bij de beoordeling van de noodzakelijkheid van de verwerking van biometrische gegevens. Ter zake vraagt de Autoriteit om uitdrukkelijk in het ontwerp te specifiëren dat indien de exploitant van een havenfaciliteit wil voorzien in de verwerking van biometrische gegevens, alle concrete elementen daaromtrent opgenomen moeten worden in de beveiligingsbeoordeling (zie ook punt 51).

53. Net zoals voor de plaatsing en het gebruik van intelligente bewakingscamera's is de grootschalige verwerking van biometrische gegevens met het oog op de unieke identificatie van de betrokkenen onderworpen aan een verplichte gegevensbeschermingseffectbeoordeling. De Memorie van toelichting bepaalt dat deze opgenomen moet worden in de beveiligingsbeoordeling. De Autoriteit neemt er akte van.

54. Op basis van de beveiligingsbeoordeling wordt een beveiligingsplan opgesteld dat ter goedkeuring moet worden voorgelegd aan de NAMB. Alleen de verwerkingen van biometrische gegevens die officieel worden goedgekeurd door de NAMB zullen effectief worden toegestaan. Daartoe specifieert de Memorie van toelichting dat uit de beveiligingsplannen uitdrukkelijk moet blijken op welke betrokken de verwerking van biometrische gegevens van toepassing is en voor welke onderdelen van de havenfaciliteit. De stellers van het ontwerp zijn van oordeel dat de verplichting om het beveiligingsplan te laten goedkeuren door een overheidsinstantie een bijkomende bescherming biedt tegen misbruiken van de in dit artikel geboden mogelijkheden.

[25] Uittreksel uit de Memorie van toelichting: *"Personen die weten waar de criminele lading zich bevindt, kunnen deze lading afzonderen om op een later tijdstip te laten ophalen. De bestuurder van een straddle carrier op een containerterminal is een voorbeeld van een werknemer die met slechte bedoelingen of onder dwang op vrij simpele wijze de lading op een vooraf afgesproken plaats kan zetten. Deze personen worden actief benaderd, al dan niet met geweld of bedreigingen, om hand- en spandiensten te leveren aan de criminele bendes. Door de controle op deze activiteiten op te voeren, wordt niet alleen de mogelijkheid tot criminele activiteiten bemoeilijkt maar wordt ook de werknemer op de havenfaciliteit in bescherming genomen. Door het gebruik van biometrie bij het behandelen van de lading kan voorzien worden dat deze straddle carriers slechts gestart kunnen worden na een verificatie van de identiteit van de bestuurder."*

Artikel 2.5.2.85 (Erkenning verwerker biometrische gegevens)

55. Om erkend te worden als verwerker van biometrische gegevens overeenkomstig de bepaling van het ontwerp moet de onderneming gevestigd zijn in de Europese Economische Ruimte, een vestigingseenheid hebben in België en een audit ondergaan door de Cel Maritieme Beveiliging en de Scheepvaartcontrole, in samenwerking met het Centrum voor Cyberveiligheid. Daarbij zal gecontroleerd worden of de onderneming voldoet aan de vereiste ISO-normen of normen die gelijkwaardig werden verklaard conform de regelgeving voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Ook zal worden nagegaan dat het door hen ontwikkelde systeem van biometrische verwerking voldoet aan de volgende vereisten[26]:

- "*1° bij het initieel inzamelen van de biometrische gegevens van een individu moeten de individuele en unieke kenmerken van de ruwe gegevens worden omgezet in gecodeerde informatie waarna de ruwe gegevens onmiddellijk wordt verwijderd*" (**betere formulering**: 1° bij de eerste inzamelingsfase van de biometrische gegevens worden de unieke en individuele kenmerken van het individu gecodeerd en als template opgeslagen, waarna de ruwe biometrische gegevens onmiddellijk verwijderd worden);
- "*2° bij het verifiëren van de identiteit van het individu wordt enkel nagegaan of de ingezamelde data tijdens het verificatieproces overeenkomt met de data opgeslagen bij het initieel inzamelen*[27]" (**betere formulering**: 2° bij het verifiëren van de identiteit van het individu wordt enkel nagegaan of de informatie die ingezameld wordt op het ogenblik dat het individu zich wenst te authentiseren overeenkomt met de template die werd opgeslagen bij de eerste inzamelingsfase);
- "*3° de opslag van de gecodeerde informatie wordt uitsluitend bewaard op een duurzaam opslagmedium dat bewaard wordt door het individu waarbij geen opslag op databases van de verwerker is toegestaan*" (**betere formulering**: 3° de template wordt uitsluitend bewaard op een duurzaam opslagmedium in het bezit van het individu waarbij geen opslag in databases van de verwerker is toegestaan).

[26] De Autoriteit stelt een aantal tekstaanpassingen voor teneinde de leesbaarheid van het artikel te verhogen.

[27] Er sloop een fout in de toelichting bij dit artikel in de Memorie van toelichting: "*bij het verifiëren van de identiteit van het individu mag niet vergeleken worden met een databank van biometrische gegevens. Het is enkel toegelaten dat de opgeslagen template van de biometrische gegevens wordt vergeleken met de informatie die* ***op de informatiedrager staat die de persoon bij zich heeft.***"

Het is daarentegen juist om te stellen dat het enkel toegelaten is om de template – dat opgeslagen is op een duurzame drager in het bezit van de betrokkene (bijvoorbeeld een toegangsbadge) – te vergelijken met de informatie die het individu tijdens de tweede inzamelingsfase (telkens wanneer het individu zich wenst te authentiseren) toont aan het systeem. Voor een uitgebreide toelichting hieromtrent verwijst de Autoriteit naar afdeling 2.3 *Het biometrische verwerkingsproces* van haar aanbeveling nr. 01/2021.

56. Ter zake stelt de Autoriteit vast dat de stellers van het ontwerp opteren voor een biometrisch systeem dat overeenkomstig de aanbeveling nr. 01/2021 van de Autoriteit de meeste waarborgen biedt tegen misbruiken en de inmenging in de rechten en vrijheden van de betrokkenen zoveel mogelijk beperkt. Volledigheidshalve vraagt de Autoriteit nog om in het ontwerp te specifiëren dat ook de biometrische gegevens die tijdens de tweede inzamelingsfase ingezameld worden (het punt 2° hierboven) niet langer mogen worden bewaard dan nodig is om deze ingezamelde gegevens te vergelijken met de template. Op die manier worden op geen enkel ogenblik biometrische gegevens (zowel ruwe gegevens als templates) bewaard in de (centrale) systemen van de verwerker. De enige gegevens die bewaard kunnen worden zijn de logs (bijvoorbeeld: naam, plaats, tijdsstip) van de biometrische toegangscontrole.

57. Na de erkenning van de onderneming wordt telkens in de periode tussen de vierentwintig en zesendertig maanden na een vorige audit een opvolgingsaudit uitgevoerd. De Autoriteit neemt er akte van.

58. Concluderend, mits inachtneming evenwel van de geformuleerde opmerkingen in dit advies en de overige richtlijnen die voortvloeien uit de aanbeveling nr. 01/2021, is de Autoriteit van oordeel dat het door het ontwerp vastgestelde wettelijk kader voor de verwerking van biometrische gegevens voldoende waarborgen kan bieden met betrekking tot de bescherming van persoonsgegevens.

Artikel 2.5.2.86 (Doeleinden, algemeen)

59. Overeenkomstig artikel 5.1.b) AVG kan de verwerking van persoonsgegevens enkel uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

60. Naast de concrete doelstellingen die werden geïdentificeerd in het kader van de verwerking van biometrische gegevens (punten 49 – 54) (en in mindere mate van het gebruik van (intelligente) bewakingscamera's (punten 39 – 48)) omschrijft dit artikel meer algemeen de doeleinden voor de verwerking van persoonsgegevens overeenkomstig hoofdstuk 2 van titel 5 van boek 2 van het Belgisch Scheepvaartwetboek:

- *"1° het garanderen van de maritieme beveiliging in havens en de havenfaciliteiten;*
- *2° het voorkomen van ongeoorloofde acties;*
- *3° het opsporen, vervolgen en bestraffen van ongeoorloofde acties;*
- *4° het garanderen van de beveiliging van de personen die werkzaam zijn in de havens en de havenfaciliteiten;*
- *5° het uitvoeren van de taken van de inlichtingendiensten;*

- *6° het controleren van de naleving van het verbod opgelegd overeenkomstig artikel 4, §3bis van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen of artikel 4.1.2.48 van het Belgisch Scheepvaartwetboek;*
- *7° het controleren van de naleving van het verbod dat personen die krachtens hoofdstuk X van de wet van 20 juli 1990 betreffende de voorlopige hechtenis de voorwaarde om zich niet in een haven of havenfaciliteit te begeven opgelegd hebben gekregen."*

61. Wat betreft het punt 2°, herneemt de Autoriteit haar opmerkingen met betrekking tot de notie 'ongeoorloofde acties' overeenkomstig punt 17.

62. Met betrekking tot de punten 3° en 5° wijst de Autoriteit erop dat het opsporen, vervolgen en bestraffen van ongeoorloofde acties en het uitvoeren van de taken van de inlichtingendiensten geen doelstellingen zijn die als zodanig nagestreefd worden door de in artikel 2.5.2.91 geïdentificeerde verwerkingsverantwoordelijken. In het licht van de centrale doelstelling van het ontwerp, met name het garanderen van de veiligheid van havens en schepen, lijkt het aangewezen om de voormelde doelstellingen af te zonderen en om te specifiëren dat de verwerkingen in dat kader door de bevoegde autoriteiten (politiediensten, gerechtelijke overheden en inlichtingendiensten) gebeuren overeenkomstig de op hen van toepassing zijnde regelgeving. Daarnaast, aangezien de verwerkingen door deze actoren niet binnen het toepassingsgebied van de AVG vallen, heeft de Autoriteit, in toepassing van het één loket principe overeenkomstig artikel 54/1 WOG, het ontwerp tevens ter advies voorgelegd aan het Controleorgaan op de politionele informatie (het COC) en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (Comité I).

63. De punten 6° en 7° voorzien dat de gegevens van de personen die een havenverbod hebben opgelopen verwerkt kunnen worden met het oog op de verplichte controle op de naleving van het havenverbod overeenkomstig artikel 2.5.2.81 (zie punten 36 – 37).

64. Volledigheidshalve vraagt de Autoriteit om in dit artikel tevens een doeleinde te identificeren aangaande de (vereiste) vorming en opleiding van bepaalde actoren (zie punten 27 – 28). Immers, zoals eerder reeds toegelicht, geeft de organisatie van dergelijke opleidingen (en examens) aanleiding tot een verwerking van persoonsgegevens van de betrokken kandidaten. Dit laat evenwel onverlet dat de vaststelling van de nadere modaliteiten van deze verwerking gedelegeerd kan worden aan de Koning.

65. Tot slot bepaalt het tweede lid van dit artikel dat *"De gegevens van de leden van de inspectiediensten*[28] *worden verwerkt met het oog op het identificeren van de opsteller van een inspectierapport of proces-verbaal."* Deze bepaling werd opgenomen naar aanleiding van een opmerking van de Raad van Staat in zijn advies 69.362/1 over een ontwerp van koninklijk besluit *tot optimalisatie van de maritieme arbeidsbepalingen*[29].

66. Mits inachtneming van de opmerkingen overeenkomstig de punten 61, 62 en 64 is de Autoriteit van oordeel dat de voorziene verwerkingen van persoonsgegevens uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

Artikelen 2.5.2.87 – 2.5.2.88 (Categorieën van betrokkenen en persoonsgegevens)

67. Artikel 5.1.c), AVG bepaalt dat persoonsgegevens toereikend, terzake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de beoogde doeleinden (principe van 'minimale gegevensverwerking').

68. De artikelen 2.5.2.87 en 2.5.2.88 bepalen respectievelijk de betrokken natuurlijke personen en de te verwerken categorieën van persoonsgegevens.

69. Van de bezoekers van havenfaciliteiten (waaronder de werknemers en bestuursleden) en de personeelsleden belast met de behandeling van de lading:

"*1° naam en voornamen;*
2° rijksregisternummer voor Belgen;
3° geboortedatum en adres voor niet-Belgen;
4° identiteitskaart- of paspoortnummer;
5° biometrische gegevens, indien van toepassing, overeenkomstig artikel 2.5.2.84;
6° doel van het bezoek;
7° aankomst- en vertrekuur en datum van het bezoek;
8° nummerplaat van wagens die de havenfaciliteit binnen- en buitenrijden;
9° foto;
10° e-mailadres."

70. In eerste instantie, hoewel de Autoriteit het belang onderschrijft van correcte identificatie en het daarbij verwerken van gegevens die voldoen aan de vereisten van kwaliteit en juistheid, benadrukt ze dat het gebruik van het Rijksregisternummer in België strikt geregeld wordt door artikel 8 van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*

[28] Zoals bedoeld in artikel 4.2.4.4.

[29] Voor bijkomende toelichting zie de Memorie van toelichting (p. 68 – 69).

(hierna: de wet van 8 augustus 1983). Het gebruik van het Rijksregisternummer is niet toegelaten zonder voorafgaandelijke machtiging, hetzij door de minister van Binnenlandse Zaken, hetzij door of krachtens een wet, een decreet of een ordonnantie. Daarenboven, in het licht van artikel 87 AVG, moet erop worden toegezien dat het gebruik van het Rijksregisternummer wordt beperkt tot de gevallen waarin dit strikt noodzakelijk is en dat technische en organisatorische maatregelen het beveiligd gebruik passend omkaderen.

71. De Autoriteit vestigt er de aandacht op de noch de formulering van artikel 2.5.2.88 noch die van artikel 2.5.2.89 een uitdrukkelijke machtiging in de zin van artikel 8 van de wet van 8 augustus 1983 constitueert.

72. Met betrekking tot de verwerking van het identiteitskaart- of paspoortnummer vraagt de Autoriteit zich af wat de meerwaarde is van dit gegeven ten aanzien van de overige categorieën van te verwerken persoonsgegevens. De geldigheidsduur van deze documenten en dus van de eraan verbonden nummers is beperkt in de tijd. Ingeval van verlies, diefstal of beschadiging zal dit nummer reeds achterhaald zijn vóór het verstrijken van de normale geldigheidsduur. Bovendien wijst de Autoriteit op de verplichting in hoofde van de verwerkingsverantwoordelijke om overeenkomstig artikel 5.1.d) AVG toe te zien op de juistheid van de gegevens en om ze zo nodig te actualiseren. Bij gebrek aan aantoonbare meerwaarde moet dit informatiegegeven worden geschrapt.

73. De (modaliteiten van de) verwerking van biometrische gegevens werd(en) reeds uitvoerig besproken in de punten 49 – 58 van dit advies.

74. Voor de voorwaarden inzake het gebruik van intelligente camera's voor nummerplaatherkenning verwijst de Autoriteit naar de punten 42 – 44 van dit advies.

75. De overige categorieën van persoonsgegevens geven in het licht van de beoogde doeleinden geen aanleiding tot bijzondere opmerkingen[30].

76. Van de PSO (de havenbeveiligingsfunctionaris[31]), de PFSO, CSO en SSO worden de volgende gegevens verwerkt:

"*1° naam en voornamen;*

2° rijksregisternummer voor Belgen;

3° geboortedatum en adres voor niet-Belgen;

[30] Ter zake verduidelijkt de Memorie van toelichting nog dat de verwerking van de foto's noodzakelijk is voor het aanmaken van toegangs- en identificatiebadges. Het e-mailadres wordt gebruikt voor de communicatie met de betrokken personen.

[31] Zie voetnoot 4.

4° e-mailadres;
5° resultaat van het examen voor PFSO's;
6° foto."

77. Betreffende het gebruik van het Rijksregisternummer verwijst de Autoriteit naar haar opmerking in punt 70. Voor het overige formuleert de Autoriteit geen bijzondere opmerkingen.

78. Van de inspecteurs mogen de volgende gegevens worden verwerkt:
"*1° naam en voornamen;*
2° identificatienummer gegeven door de overheidsdienst waarvoor de inspecteur werkt;
3° foto."

79. Teneinde de coherentie van de tekst te verhogen vraagt de Autoriteit om het woord '*inspecteurs'* in artikel 2.5.2.88, §3 te vervangen door '*leden van de inspectiediensten bedoeld in artikel 4.2.4.4'* overeenkomstig artikel 2.5.2.87. Voor het overige geen opmerkingen met betrekking tot de te verwerken persoonsgegevens.

80. Tot slot, van de personen die een verbod kregen overeenkomstig artikel 4, §3*bis* van de Drugswet of artikel 4.1.2.48 van het Belgisch Scheepvaartwetboek en van de personen die krachtens hoofdstuk X van de wet van 20 juli 1990 *betreffende de voorlopige hechtenis* de voorwaarde om zich niet in een haven of havenfaciliteit te begeven opgelegd hebben gekregen, mogen de volgende gegevens verwerkt worden:
"*1° naam en voornamen;*
2° rijksregisternummer voor Belgen[32]*;*
3° datum tot wanneer het verbod van kracht is;
4° havens en havenfaciliteiten waar het verbod van kracht is."

81. De Autoriteit neemt er akte van.

Artikel 2.5.2.89 (Toegang)

82. Dit artikel bepaalt: *"De leden van de NAMB, het betrokken LCMB, de Cel Maritieme Beveiliging, het openbaar ministerie, de inlichtingendiensten en de inspectiediensten bedoeld in artikel 4.2.4.4 hebben toegang tot de gegevens bedoeld in artikel 2.5.2.**~~82~~ 84 88** en voor de doeleinden bedoeld in artikel 2.5.2.**~~82~~ 86**[33]*.*

[32] Zie opnieuw punt 70.

[33] In punt 34 werd reeds gewezen op de foutieve verwijzingen in het ontwerp.

In afwijking van het eerste lid, hebben enkel de verwerkingsverantwoordelijke, de verwerker en de inlichtingendiensten en federale en lokale politie toegang tot de biometrische gegevens."
De Memorie van toelichting voegt hieraan toe dat het een exhaustieve oplijsting betreft van de overheidsdiensten die belast zijn met het toezicht en de controle op de naleving van de regelgeving inzake maritieme bewaking.

83. Zoals hierboven reeds toegelicht (zie punten 33 – 35) is het noodzakelijk dat de modaliteiten van de toegang tot de persoonsgegevens beter afgestemd moeten worden op de regelgeving betreffende het ISPS-platform waarlangs deze toegang vermoedelijk plaats zal vinden.

84. Daarnaast vraagt de Autoriteit zich af tot welke biometrische gegevens de inlichtingendiensten en de federale en lokale politie toegang kunnen krijgen. Immers, zoals dit volgt uit artikel 2.5.2.85 – en tevens wordt vereist door de Autoriteit – moeten de ruwe biometrische gegevens, bij de eerste inzamelingsfase onmiddellijk omgezet worden in een gecodeerde template die enkel bewaard wordt op een duurzaam opslagmedium in het exclusieve bezit van de betrokkene. Hoewel de Autoriteit logischerwijze onderschrijft dat deze gegevens verwerkt zullen worden door de verwerkingsverantwoordelijke en de verwerkers met het oog op de organisatie en het beheer van de biometrische toegangscontrole, benadrukt zij dat in deze context enkel de volgende gegevens bewaard mogen worden:
    - de loggegevens van de biometrische toegangscontrole (zonder dat deze biometrische gegevens kunnen bevatten);
    - het biometrische template in het exclusieve bezit van de betrokken (bijvoorbeeld de toegangs- of identificatiebadge).

    Rekening houdend met het bovenstaande is de Autoriteit van oordeel dat de voormelde passage geen enkele meerwaarde heeft (en bovendien verwarring creëert) en bijgevolg moet worden geschrapt.

85. De Autoriteit benadrukt dat het template onder geen beding gekopieerd, noch buiten het duurzame opslagmedium bewaard mag worden (behoudens natuurlijk tijdens de effectieve verificatie van de identiteit van de betrokkene bij een toegangscontrole, mits inachtneming van de opmerking in punt 56).

Artikel 2.5.2.90 (Bewaringstermijn)

86. Krachtens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

87. Daartoe wordt in artikel 2.5.2.90 het volgende bepaald: "*De gegevens bedoeld in artikel 2.5.2.88 worden bewaard gedurende de periode bepaald in het beveiligingsplan en kunnen nooit de periode van* ***10 jaar*** *overschrijden.*
In afwijking van het eerste lid, mogen ***de biometrische gegevens*** *slechts bewaard blijven gedurende een termijn van 2 jaar na het bezoek aan een havenfaciliteit of nadat de betrokkene geen toegang meer heeft tot de netwerk- en informatiesystemen.*
In afwijking van het eerste lid worden ***de gegevens van de personen bedoeld in artikel 2.5.2.87, 4° en 5°****, onmiddellijk verwijderd nadat het havenverbod is afgelopen of opgeheven."*

88. Met betrekking tot de 'standaard' bewaartermijn van 10 jaar specifieert de Memorie van toelichting dat een dergelijke termijn noodzakelijk is in het kader van de handhaving van de regelgeving, met inbegrip van de gerechtelijke procedures. De Autoriteit neemt er akte van, doch vraagt aan de NAMB om bij de goedkeuring van de beveiligingsplannen erop toe te zien dat de toepassing van voormelde bewaartermijn steeds gerechtvaardigd is. Wanneer blijkt dat voor sommige gegevens een kortere termijn kan worden gehanteerd moet overeenkomstig gehandeld worden.

89. Vervolgens voorziet artikel 2.5.2.90 in een bijzondere bewaartermijn voor de biometrische gegevens van de betrokkenen. Zoals hierboven reeds werd toegelicht moeten de ruwe biometrische gegevens na de eerste inzamelingsfase onmiddellijk verwijderd worden nadat zij werden omgezet in een gecodeerde biometrische template. Tevens verzocht de Autoriteit in dit kader om te specifiëren dat ook de gegevens van de tweede inzamelingsfase (de feitelijke verificatie) niet langer mogen worden bewaard dan nodig is om ze te vergelijken met de template[34]. Alleen op de toegangsbadge, die enkel in het bezit is van de betrokkene, wordt een biometrisch gegeven bewaard (de template).

90. Aldus stelt de Autoriteit zich vragen bij de voorziene bewaartermijn van maximaal twee jaar nadat een bepaalde persoon voor het laatst toegang heeft gehad tot de fysieke plaatsen of nadat hij geen toegang meer heeft tot de netwerk- en informatiesystemen. Een dergelijke termijn kan immers niet gehanteerd worden wanneer de betrokken persoon zijn toegangsbadge niet inlevert. De Autoriteit vraagt daarentegen om in het ontwerp te specifiëren dat de badges (waarop een biometrisch template werd opgeslagen), indien mogelijk, onmiddellijk vernietigd worden nadat de betrokken personen geen toegang meer hebben tot de geviseerde fysieke plaatsen of de netwerk- en informatiesystemen. Indien de vernietiging van de badge om welke reden dan ook niet mogelijk zou zijn, dan moet minstens worden voorzien in de mogelijkheid om deze badge te 'deactiveren' ten einde het verdere gebruik ervan onmogelijk te maken. Op dat ogenblik dient deze persoon

[34] Zie punt 56.

hoe dan ook geschrapt te worden uit de lijst met personen die toegang hebben tot de voormelde plaatsen (dit om te vermijden dat een persoon die valselijk beweert zijn badge kwijt te zijn alsnog toegang kan krijgen). Dit laat uiteraard onverlet de standaard bewaartermijn die kan gelden ten aanzien van de loggegevens van de biometrische toegangscontrole.

91. Een tweede uitzondering betreft de gegevens van de personen aan wie een havenverbod werd opgelegd. De Autoriteit neemt er akte van dat deze gegevens onmiddellijk worden geschrapt na afloop van het havenverbod. Daartoe kan gewerkt worden aan de hand van een geautomatiseerd systeem dat de gegevens verwijdert zodra de vervaldatum werd bereikt.

Artikel 2.5.2.91 (Verwerkingsverantwoordelijke)

92. Overeenkomstig artikel 4.7) AVG is de verwerkingsverantwoordelijke elke natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De Autoriteit herinnert er bovendien aan dat de aanwijzing of kwalificatie als verwerkingsverantwoordelijke in het licht van de feitelijke omstandigheden gepast moet zijn. Met andere woorden, voor elke verwerking van persoonsgegevens moet worden nagegaan wie feitelijk het omschreven doel nastreeft en de effectieve controle uitoefent over de verwerking[35].

93. Artikel 2.5.2.91 bepaalt:
"De PFSO is de verwerkingsverantwoordelijke voor de bezoekers van een havenfaciliteit[36]*.*
De NAMB is de verwerkingsverantwoordelijke voor de PSO, PFSO, CSO, SSO en de inspecteurs.
De NAMB is de verwerkingsverantwoordelijke voor de personen bedoeld in artikel 2.5.2.87, 4° en 5°."

94. In eerste instantie vraagt de Autoriteit om in dit artikel, naar analogie met artikel 2.5.2.90, steeds de volgende verduidelijking op te nemen: 'De … is de verwerkingsverantwoordelijke voor de gegevens van de … **bedoeld in artikel 2.5.2.88, §… die worden verwerkt voor de doeleinden bedoeld in artikel 2.5.2.86**'.

95. Vervolgens merkt de Autoriteit op dat de PFSO aangeduid wordt als de verwerkingsverantwoordelijke voor de gegevens van de bezoekers (waaronder de personeelsleden en de bestuurders) van een havenfaciliteit. Hieruit lijkt te volgen dat de onderneming waar de PFSO werd aangesteld (de exploitant van de havenfaciliteit) louter optreedt als verwerker in de

[35] Zie ter zake ook de Richtsnoeren 07/2020 *over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG*. Te raadplegen via : https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_nl.pdf.

[36] De bijzonderheden met betrekking tot de verwerker van de biometrische gegevens werden reeds besproken in punt **Error! Reference source not found.** e.v.

zin van artikel 4.8) AVG. Artikelen 5.1, f) en 24 AVG verplichten de verwerkingsverantwoordelijke om de nodige passende technische en organisatorische maatregelen te nemen om een op het risico van misbruik afgestemd beveiligingsniveau te waarborgen. Daarenboven vereist artikel 28.1 AVG dat de verwerkingsverantwoordelijke uitsluitend beroep kan doen op verwerkers die afdoende garanties bieden opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

96. Ter zake betwijfelt de Autoriteit evenwel dat de PFSO, die in voorkomend geval een werknemer of bestuurder is van de exploitant van de havenfaciliteit, effectief optreedt als verwerkingsverantwoordelijke. De PFSO kiest immers niet welke onderneming de havenfaciliteit mag uitbaten, noch lijkt het aannemelijk dat hij het doel en, belangrijker, de middelen van de verwerking eigenhandig bepaalt. Bovendien zou dit impliceren dat bij elke schending van de AVG de PFSO persoonlijk aansprakelijk kan worden gesteld, hetgeen, in het bijzonder als de PFSO een werknemer is van de exploitant, niet valt te rechtvaardigen. Derhalve is de Autoriteit van oordeel dat de exploitanten van de havenfaciliteiten aangemerkt moeten worden als verwerkingsverantwoordelijken. Dit laat onverlet de verplichting om een PFSO aan te stellen overeenkomstig de bepalingen van het ontwerp. De PFSO kan binnen de onderneming aangeduid worden als centraal aanspreekpunt inzake gegevensbescherming.

97. De aanduiding van de NAMB als verwerkingsverantwoordelijke voor de PSO, PFSO, CSO, SSO en de inspecteurs geeft geen aanleiding tot bijzondere opmerkingen inzake de bescherming van persoonsgegevens.

98. Tot slot verduidelijkt de Memorie van toelichting dat voor wat betreft de personen met een havenverbod de verantwoordelijkheid van de NAMB beperkt is tot het controleren van het verbod. De eigenlijke verwerking van de beslissingen, vonnissen of arresten die een dergelijk havenverbod opleggen, blijft binnen de werkingssfeer van de FOD Justitie. De Autoriteit neemt er akte van.

Artikelen 2.5.2.92 – 2.5.2.95 (Inperking van de rechten)

99. De voormelde artikelen voorzien in een afwijking van het recht op informatie, inzage, rectificatie en beperking van de verwerking voor wat betreft de verwerkingen die de voorbereiding, de organisatie het beheer en de opvolging van de gevoerde onderzoeken, met inbegrip van gerechtelijke onderzoeken en de eventuele toepassing van een administratieve sanctie, tot doel hebben.

100. Elke beperking van de rechten van betrokkenen krachtens de AVG moet niet alleen een van de in artikel 23.1 AVG genoemde doeleinden nastreven, maar ook voldoen aan de in artikel 23.2

AVG voorgeschreven vormen[37]. Bovendien moet elke beperking van de rechten van de betrokkenen beperkt blijven tot wat strikt noodzakelijk is, zowel wat de reikwijdte als wat de duur betreft[38]. Hoewel de Autoriteit begrijpt dat er voor controle- en inspectieverwerkingen kan worden voorzien in afwijkingen van bepaalde door de AVG gewaarborgde rechten (teneinde de controles en de gevoerde onderzoeken niet in het gedrang te brengen), is zij van oordeel dat de huidige verwoording van de ter advies voorgelegde artikelen niet verenigbaar is met voorwaarden overeenkomstig artikel 23 AVG en de vereisten inzake rechtszekerheid en voorzienbaarheid in hoofde van de betrokkenen[39].

101. In de eerste plaats moeten de verwerkingsverantwoordelijken die deze afwijkingen genieten, uitdrukkelijk worden vermeld in het ontwerp.

102. Vervolgens benadrukt de Autoriteit dat het overeenkomstig artikel 23.2 AVG de taak is van de stellers van het ontwerp om de reikwijdte van de beperkingen te specificeren, niet alleen op vlak van rechten waarvan wordt afgeweken, maar ook op vlak van de limieten van de beoogde beperkingen. In dit verband beveelt de Autoriteit aan, zonder exhaustief te willen zijn, te specifiëren dat de afwijkingen van de rechten van de betrokkenen alleen gelden gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of een onderzoek (met inbegrip van de voorbereidende handelingen tot hoogstens één jaar vanaf de ontvangst van het verzoek om uitoefening van het recht[40]) en gedurende de periode die nodig is voor de vervolging ter zake, voor zover de uitoefening van de rechten afbreuk zou doen aan de behoeften van de controle, het onderzoek of de voorbereidende handelingen.

103. Tot slot, teneinde de voormelde artikelen van het ontwerp verenigbaar te maken met artikel 23.2 AVG moet bovendien worden voorzien in soortgelijke garanties als die waarin hoofdstuk 5/1 *Sociaal Strafwetboek* voorziet. Deze afwijkingen en garanties voor de rechten en vrijheden van de betrokkenen werden immers reeds goedgekeurd door de Autoriteit in het advies nr. 34/2018[41]. Er

---

[37] Zie in dit kader de EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR (vooralsnog enkel beschikbaar in het Engels). Te raadplegen via: https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf.

[38] Zie ook verschillende adviezen van de Autoriteit: advies nr. 34/2018 van 11 april 2018 *over een voorontwerp van wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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*, meer bepaald de overwegingen 36 tot 38; advies nr. 41/2018 van 23 mei 2018 *over een voorontwerp van wet houdende diverse financiële bepalingen*; advies nr. 88/2018 van 26 september 2018 *over het ontwerp van besluit van de Vlaamse Regering houdende aanpassing van de besluiten van de Vlaamse Regering aan de 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).*

[39] EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, p. 8: *"the domestic law must be sufficiently clear in its terms to give individuals an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such restrictions."*

[40] Teneinde een redelijke beperking in de tijd voor de afwijking te garanderen.

[41] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-34-2018.pdf.

wordt gedacht aan: aanduiden van de feitelijke of juridische gronden waarop het besluit tot weigering van de uitoefening van een recht van de betrokkene is gebaseerd, het in kennis stellen van de betrokkenen van de afwijzing van hun verzoek en de redenen daarvoor, tenzij dit het doel van de controle in gevaar zou brengen, het in kennis stellen van de betrokkenen die hun rechten hebben willen uitoefenen van de opheffing van de afwijking na de afronding van de controle, het in kennis stellen van de betrokkenen van de rechtsmiddelen waarover ze in dat verband beschikken, …

c. <u>Artikel 21 van het ontwerp</u>

104. Artikel 21 van het ontwerp vult boek 4 van het Belgische Scheepvaartwetboek aan met een titel 6 luidende: *"Bijzondere bepalingen voor de Noordzee".* Het betreft een *lex specialis* regime ten aanzien van het plaatsen van bewakingscamera's in de Noordzee door private personen en overheden aangezien de Camerawet hier niet kan worden toegepast[42]. Desalniettemin hebben de stellers van het ontwerp geopteerd voor een begrippenkader[43] en structuur in overeenstemming met de voormelde wet, hetgeen de transparantie en de voorzienbaarheid van de regelgeving ten goede komt.

105. De bepalingen van deze titel zijn van toepassing op de plaatsing en het gebruik van camera's in de Belgische territoriale zee en de Exclusief Economische Zone voor de volgende doeleinden[44]:

"1° misdrijven tegen personen of goederen te voorkomen, vast te stellen of op te sporen;
2° het mariene milieu te beschermen;
3° wetenschappelijk onderzoek;
4° de scheepvaartveiligheid garanderen;
5° de beveiliging van de kunst- en bouwwerken, kabels en pijpleidingen te garanderen;
6° de beveiliging van de Belgische maritieme zones garanderen;
7° het behoud van de levende rijkdommen."

Behoudens de opmerkingen hieronder is de Autoriteit van oordeel dat deze doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.

---

[42] Verscheidene voorwaarden die door de Camerawet worden gesteld hebben immers geen enkele betekenis in deze context: de vereiste toelating door de gemeente, het plaatsen van pictogrammen en het afsluiten door middel van een fysieke omheining van private domeinen om camera's voor privaat gebruik te kunnen installeren, …

[43] Artikel 4.6.1.2, naar analogie met artikel 2 van de Camerawet, hanteert dezelfde definities voor de begrippen camera, vaste of mobiele camera en intelligente camera.

[44] Artikel 4.6.1.4.

Artikel 4.6.1.6 (Gebruik van vaste camera's in de territoriale zee)

106. *Het initiatief tot het plaatsen van één of meer vaste camera's* – camera's die tijdens de observatie op een vaste plaats blijven om vanaf deze locatie te filmen – *wordt genomen door de verwerkingsverantwoordelijke, die enkel een openbare overheid kan zijn*. Daartoe richt de verwerkingsverantwoordelijke de aanvraag voor het installeren van deze camera's aan de Cel Maritieme Beveiliging en verduidelijkt minstens volgende punten:

"*1° locatie van het plaatsen van de camera;*

2° de perimeter;

3° het doeleinde van het gebruik van de camera;

4° de specificaties van de camera;

5° de voorgestelde bewaringstermijn die de maximale van duur zoals bepaald ***in paragraaf 5, tweede lid***[45]*, niet te boven mag gaan;*

6° de wijze waarop de verwerking van de gegevens gebeurt."

De Cel Maritieme Beveiliging bezorgt het dossier, samen met het advies van het Maritiem Informatiekruispunt[46] (hierna: MIK) aan de Minister bevoegd voor maritieme mobiliteit die beslist over de plaatsing en de modaliteiten van de camera's. Eens de camera's worden geplaats maakt de Cel Maritieme Beveiliging de plaatsing van ervan bekend via een Bericht aan Zeevarenden en een publicatie op haar website.

107. De Memorie van toelichting verduidelijkt dat deze ministeriële beslissing in de plaats treedt van de toelating door de gemeente die wordt vereist voor de plaatsing van camera's op het vaste land[47]. De publicatie van de gegevens van de camera via de bekende nautische publicaties vervangt de het pictogram dat krachtens de Camerawet moet worden geplaats om aan te tonen dat er camerabewaking plaatsvindt.

108. Met betrekking tot de voormelde aanvraagprocedure formuleert de Autoriteit de volgende opmerkingen:

- het lijkt zonder meer aangewezen om te voorzien in een gestandaardiseerd aanvraagformulier. De vorm en de inhoud daarvan kunnen desgevallend worden vastgesteld

[45] De Autoriteit stelt vast dat geen artikel 4.6.1.6, §5, tweede lid bestaat. De Autoriteit vermoedt dat naar paragraaf 7 moet verwezen worden.

[46] Het Maritiem Informatiekruispunt zoals bedoeld in artikel 3, 7°, van het Samenwerkingsakkoord *tussen de Federale Staat en het Vlaamse Gewest betreffende de oprichting van en de samenwerking in een structuur kustwacht* van 8 juli 2005 is samengesteld uit vier partners, met name Defensie, de Scheepvaartpolitie, de Algemene Administratie Douane en Accijnzen, en DG Scheepvaart.

[47] Artikel 5 van de Camerawet.

door de Koning[48]. In het bijzonder de noties '*specificaties van de camera'* en '*wijze waarop de verwerking van gegevens gebeurt*' laten een te ruime marge voor subjectieve invulling;

- nergens in het ontwerp worden modaliteiten van de geïmpliceerde adviesverplichting in hoofde van het MIK geregeld, dit moet worden rechtgezet. Indien deze verplichting voortvloeit uit een andere wettelijke bepaling moet daarnaar worden verwezen;
- naar analogie met de artikelen 2.5.2.19 en 2.5.2.35 moet voorzien worden in een maximale geldigheidsduur van de goedkeuring door de minister, waarna een nieuwe aanvraag moet worden ingediend.

109. Paragraaf 4 van dit artikel bepaalt *"De verwerkingsverantwoordelijke houdt een register bij met de beeldverwerkingsactiviteiten van de camera's uitgevoerd onder zijn verantwoordelijkheid. De Koning bepaalt de inhoud van dit register, de modaliteiten en de bewaartermijn ervan."* Ter zake vraagt de Autoriteit zich af hoe dit register zich verhoudt ten opzichte van het register van de verwerkingsactiviteiten dat de verwerkingsverantwoordelijke overeenkomstig artikel 30 AVG reeds moet bijhouden[49]. Een verduidelijking in die zin kan bijvoorbeeld opgenomen worden in de Memorie van toelichting. In elk geval benadrukt de Autoriteit dat de Koning met betrekking tot de inhoud van het register geen afbreuk kan doen aan de minimale vereisten die artikel 30 AVG naar voren schuift[50].

110. Paragraaf 5 bepaalt dat het bekijken van deze beelden in real time enkel toegestaan is door de diensten bedoeld in artikel 4.2.4.4/1, namelijk de Scheepvaartcontrole, de Cel Maritieme Beveiliging, de leden van de NAMB, de Algemene Administratie Douane en Accijnzen, het Ministerie van Landsverdediging, de federale politie en het Belgische Mathematisch Model voor de Noordzee. Naar analogie met de bepalingen van de Camerawet inzake het in real time bekijken van beelden van bewakingscamera's, moet in het ontwerp worden gespecifieerd dat een dergelijke toegang uitsluitend toegestaan is opdat de bevoegde diensten, binnen het kader van hun wettelijke opdracht, onmiddellijk kunnen ingrijpen bij misdrijf of schade en deze diensten in hun optreden optimaal kunnen worden gestuurd, of teneinde bewijzen te verzamelen van feiten die een misdrijf opleveren of schade veroorzaken en daders, getuigen of slachtoffers op te sporen en te identificeren. Indien de stellers van het ontwerp bijkomende doeleinden identificeren voor het in real time bekijken van de beelden (bijvoorbeeld in het kader van wetenschappelijk onderzoek) dient dit uitdrukkelijk opgenomen te worden in het ontwerp.

---

[48] Naar analogie met het formulier dat door de verwerkingsverantwoordelijke moet worden overgemaakt aan de politiediensten overeenkomstig de Camerawet.

[49] Ongeacht of de betrokken verwerkingsverantwoordelijke meer of minder dan 250 personen in dienst heeft, is de Autoriteit van oordeel dat de geviseerde verwerkingen van persoonsgegevens een risico inhouden voor de rechten en vrijheden van de betrokkenen.

[50] Eenzelfde opmerking gaat op voor de gelijkaardige bepalingen in de Camerawet. Zie in dat kader ook punt 23 van het advies nr. 53/2017 van de Commissie voor de bescherming van de persoonlijke levenssfeer, rechtsvoorganger van de Autoriteit.

111. Vervolgens bepaalt paragraaf 6: *"Het opnemen van de beelden is uitsluitend toegestaan teneinde bewijzen te verzamelen van feiten die een misdrijf opleveren of schade veroorzaken en daders, getuigen of slachtoffers op te sporen en te identificeren."* De Autoriteit is van oordeel dat deze bepaling verkeerdelijk de indruk geeft dat de camera's die worden geplaats overeenkomstig dit hoofdstuk enkel aangewend kunnen worden om bewijzen te verzamelen van feiten die een misdrijf opleveren of schade veroorzaken en daders, getuigen of slachtoffers op te sporen en te identificeren. Ook in het geval dat de verwerkingsverantwoordelijke een ander doeleinde voor de plaatsing van camera's overeenkomstig artikel 4.6.1.4 heeft opgegeven[51] (bijvoorbeeld wetenschappelijk onderzoek) moet het mogelijk zijn om beelden op te nemen en te analyseren. Bovendien wijst de Autoriteit erop dat een onderscheid moet worden gemaakt tussen camerabeelden die wel of niet aangemerkt moeten worden als persoonsgegevens. Immers, indien er geen sprake is van een verwerking van persoonsgegevens moeten de bepalingen van de AVG logischerwijze niet in acht worden genomen. Als dusdanig vraagt de Autoriteit om deze bepaling als volgt aan te passen: 'Het opnemen van de beelden **die aanleiding geven tot een verwerking van persoonsgegevens** is uitsluitend toegestaan **voor de verwezenlijking van de doelstellingen bedoeld in artikel 4.6.1.4.**'

112. Eenzelfde opmerking gaat op voor wat betreft de bewaartermijn van de beelden overeenkomstig paragraaf 7: *"Indien deze beelden geen bijdrage kunnen leveren tot het bewijzen van een misdrijf, van schade of van overlast of tot het identificeren van een dader, een verstoorder van de openbare orde, een getuige of een slachtoffer, worden zij niet langer dan zes maanden bewaard."* Vooreerst lijkt het aangewezen om te specifiëren dat enkel de beelden die gekwalificeerd moeten worden als persoonsgegevens onderworpen zijn aan een bewaartermijn. Daarnaast wordt opnieuw geen rekening gehouden met de overige doelstellingen die rechtmatig kunnen worden nagestreefd door middel van deze camera's. Tot slot, en dit ter zijde, is het voor de Autoriteit niet duidelijk op welk ogenblik het vaststaat dat de beelden geen bijdrage kunnen leveren tot het bewijzen van een misdrijf, van schade of van overlast of tot het identificeren van de geviseerde personen, zodat de 'bewaartermijn' van zes maanden begint te lopen. De Autoriteit vraagt aldus om paragraaf 7 als volgt aan te passen: 'De beelden **die aanleiding geven tot een verwerking van persoonsgegevens** worden niet langer bewaard dan strikt noodzakelijk voor de verwezenlijking van de doelstellingen zoals bedoeld in artikel 4.6.1.4, zonder dat deze termijn … jaar kan overschrijden.' Het is aan de stellers van het ontwerp of de verwerkingsverantwoordelijken om in functie van het beoogde doeleinde, een passende maximale bewaringstermijn vast te stellen.

[51] Het doeleinde voor het plaatsen van de camera's moet tevens uitdrukkelijk worden vastgesteld bij de aanvraag én in register van de verwerkingsactiviteiten.

113. Tot slot bepaalt paragraaf 8 dat in afwijking van het principe dat alleen openbare overheden kunnen optreden als verwerkingsverantwoordelijke, ook de exploitant van een kunst- of bouwwerk, kabel of pijpleiding een aanvraag kan indien voor het plaatsen van bewakingscamera's in de territoriale zee op voorwaarde dat:
"1° het gebruik van de camera's is opgenomen in het beveiligingsplan bedoeld in artikel 2.5.2.64; of
2° het gebruik van de camera tot doel heeft de naleving van de veiligheidszone vastgesteld overeenkomstig het koninklijk besluit van 4 februari 2020 tot instelling van veiligheidszones in de zeegebieden onder Belgische rechtsbevoegdheid."

In dit geval zijn de paragrafen 2 – 4 en 6 – 7 van artikel 4.6.1.6 *mutatis mutandis* van toepassing. De Autoriteit neemt er akte van.

Artikelen 4.6.1.7 – 4.6.1.8 (Mobiele camera's in de territoriale zee/ camera's in de Exclusief Economische Zone)

114. De artikelen 4.6.1.7 en 4.6.1.8 bepalen respectievelijk dat mobiele camera's enkel geïnstalleerd kunnen worden in de territoriale zee door een overheid bedoeld in artikel 4.1.4.4/1 overeenkomstig de modaliteiten in artikel 4.6.1.6 en dat het gebruik van vaste of mobiele camera's in de Exclusief Economische Zone toegelaten is overeenkomstig de regelgeving die geldt voor de territoriale zee, op voorwaarde dat de aanvrager (die de camera's wil plaatsen) kan aantonen dat de camera wordt aangewend voor één van de rechten bedoeld in artikel 56[52] of 60[53] van het VN-Zeerechtenverdrag. De Autoriteit neemt er akte van en verwijst naar de bespreking van artikel 4.6.1.6.

Artikel 4.6.1.9 (Heimelijk gebruik van camera's)

115. Overeenkomstig dit artikel is het heimelijk gebruik (lees: zonder voorafgaande toestemming van de betrokkenen) van camera's verboden. Het betreden van een plaats zoals aangegeven overeenkomstig artikel 4.6.1.6, §3 geldt als het geven van toestemming. Zowel de formulering als het uitgangspunt van dit artikel zijn bijzonder problematisch. In eerste instantie benadrukt de

[52] Dit artikel bepaalt dat in de exclusief economische zone de kuststaat bezit: *"soevereine rechten ten behoeve van de exploratie en exploitatie, het behoud en het beheer van de natuurlijke rijkdommen, levend en niet-levend, van de wateren boven de zeebodem en van de zeebodem en de ondergrond daarvan, en met betrekking tot andere activiteiten voor de economische exploitatie en exploratie van de zone, zoals de opwekking van energie uit het water, de stromen en de winden; rechtsmacht zoals bepaald in de desbetreffende bepalingen van dit verdrag ten aanzien van de bouw en het gebruik van kunstmatige eilanden, installaties en inrichtingen, wetenschappelijk zeeonderzoek en de bescherming en het behoud van het mariene milieu; andere rechten en plichten, bepaald in dit verdrag."*

[53] Dit artikel heeft betrekking op het uitsluitende recht van de kuststaat om te bouwen en om de bouw, de werkzaamheden en het gebruik te machtigen en regelen van: *"kunstmatige eilanden; installaties en inrichtingen voor de doeleinden bepaald in artikel 56 en voor andere economische doeleinden; en installaties en inrichtingen die inbreuk kunnen maken op de uitoefening van de rechten van de kuststaat in de exclusief economische zone."*

Autoriteit dat het 'betreden van een dergelijke plaats' geenszins aanleiding kan geven tot een geldige toestemming in de zin van de AVG[54]. Daarnaast wijst de Autoriteit erop dat de toestemming als rechtsgrond voor de verwerking hier hoe dan ook niet aan de orde is (kan zijn). De door deze camera's geïnitieerde verwerkingen van persoonsgegevens steunen immers op artikel 6.1.e) AVG (het algemeen belang). Beter is aldus om te stellen dat 'elke plaatsing (elk gebruik) van camera's in de territoriale zee of de exclusief economische zone in strijd met de bepalingen overeenkomstig de artikelen 4.6.1.4 en 4.6.1.6 – 4.6.1.8 verboden is'. De Autoriteit verzoekt om het artikel nuttig te wijzigen in die zin.

Artikel 4.6.1.10 (Intelligente camera's)

116. Aangezien nergens blijkt waarom camerabeelden nodig zijn voor de automatische herkenning van vaartuigen – immers, zoals aangegeven door de aanvrager, gebeurt de automatische herkenning via een AIS-transponder (radiogolven) – herneemt de Autoriteit haar opmerkingen overeenkomstig de punten 45 – 46. Indien een vaartuig, ten onrechte, niet beschikt over een AIS-transponder, kunnen gewone bewakingscamera's volstaan teneinde het schip en desgevallend elke overtreding vast te leggen. Het artikel dient geschrapt te worden.

Artikel 4.6.1.11 (Non-discriminatie)

117. Dit artikel bepaalt: *"De camera's mogen noch beelden opleveren die de intimiteit van een persoon schenden, noch gericht zijn op het inwinnen van informatie over de filosofische, religieuze, politieke, syndicale gezindheid, etnische of sociale origine, het seksuele leven of de gezondheidstoestand."* Bijkomend volgt uit de Memorie van toelichting dat deze bepaling werd overgenomen uit de Camerawet en naar analogie moet worden geïnterpreteerd.

118. De Autoriteit betwijfelt evenwel de meerwaarde van dit artikel. Immers, zoals reeds toegelicht onder punt 115 wordt het gebruik van bewakingscamera's in strijd met de artikelen 4.6.1.4 en 4.6.1.6 – 4.6.1.8 geacht verboden te zijn. Geen enkel doeleinde zoals omschreven in artikel 4.6.1.4 rechtvaardigt het gebruik van camera's die beelden zouden opleveren in de zin van dit artikel. Daarnaast brengt de Autoriteit in herinnering dat overeenkomstig artikel 9.1 AVG elke verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en elke verwerking van gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid verboden zijn, tenzij een uitzondergrond overeenkomstig

[54] Artikel 4.11) AVG: *"toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;"*

artikel 9.2 AVG voorhanden is. Aangezien deze bepaling aldus louter de reeds van kracht zijnde regelgeving herhaalt[55], vraagt de Autoriteit om dit artikel te schrappen.

Artikel 4.6.1.12 (Recht van toegang)

119. Dit artikel bepaalt het volgende: "*Iedere gefilmde persoon heeft een recht van toegang tot de beelden.*

De gefilmde persoon richt hiervoor een verzoek aan de verwerkingsverantwoordelijke. Dit verzoek bevat voldoende gedetailleerde aanwijzingen om de betrokken beelden precies te kunnen lokaliseren.

Wanneer de gefilmde persoon aanspraak kan maken op het recht om een kopie te verkrijgen overeenkomstig artikel 15, 3, van de AVG kan de verwerkingsverantwoordelijke het verzoek tot toegang inwilligen, door aan de gefilmde persoon de beelden te laten bekijken, zonder een kopie van de beelden te verstrekken, teneinde te waarborgen dat:

1° de rechten en vrijheden van andere zoals voorzien door artikel 15, 4, van de AVG niet in het gedrang komen;

2° de openbare veiligheid of de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, met toepassing van artikel 23, 1, c) en d), van de AVG niet in gevaar wordt gebracht."

120. Voormeld artikel beoogt aldus te voorzien in een beperking van het recht van de gefilmde persoon om een kopie te krijgen van de beelden wanneer dit afbreuk zou doen aan de rechten en vrijheden van anderen of de openbare veiligheid of de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten in gevaar wordt gebracht. In eerste instantie stelt de Autoriteit vast dat het punt 1° een schending betreft van het overschrijfverbod van de AVG[56]. Deze bepaling moet geschrapt worden. Daarnaast vraagt de Autoriteit zich af of het niet opportuun is om, naar analogie met de artikelen 2.5.2.92 – 2.5.2.95, te voorzien in een bredere inperking van de rechten van de betrokkenen voor wat betreft de gegevensverwerkingen aan de hand van camera's die de voorbereiding, de organisatie, het beheer en de opvolging van de gevoerde onderzoeken, met inbegrip van gerechtelijke onderzoeken en de eventuele toepassing van een administratieve sanctie, tot doel hebben. In ieder geval, het spreekt voor zich dat de opmerkingen

[55] Hetgeen bovendien een schending van het overschrijfverbod van Europese verordeningen impliceert; de rechtstreekse toepasselijkheid van Europese verordeningen houdt een verbod in om deze in nationaal recht om te zetten omdat een dergelijke procedure *"een dubbelzinnigheid kan creëren over zowel de juridische aard van de toepasselijke bepalingen als het tijdstip van hun inwerkingtreding".* Zie in dit kader: HJEU, 7 februari 1973, Commissie c. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Zie ook: HJEU, 10 oktober 1973, Fratelli Variola S.p.A. c. Italiaanse Belastingsdienst (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11; HJEU, 31 januari 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99, §§ 24-26.

[56] Overeenkomstig artikel 15.4 AVG wordt het recht om een kopie te verkrijgen reeds ingeperkt indien zulks afbreuk doet aan de rechten en vrijheden van anderen.

van de Autoriteit overeenkomstig de punten 100 – 103 *mutatis mutandis* gelden ten aanzien van deze beperkingen. Dit artikel moet nuttig gewijzigd worden in die zin.

OM DEZE REDENEN,
de Autoriteit

is van oordeel dat de volgende wijzigingen van het ontwerp zich opdringen:

- preciseren van de notie 'ongeoorloofde actie' (punten 17 – 26);
- verduidelijken welke actoren concreet instaan voor de verwezenlijking van welke doeleinden van het ISPS-platform, met inbegrip van de verwerkingen van persoonsgegevens in dat kader (punten 33 – 35, 38 en 83);
- verbeteren van de verwoording van het doeleinde inzake het havenverbod van het ISPS-platform (punt 37);
- uitklaren van de problematiek inzake het gebruik van intelligente camera's voor nummerplaatherkenning in zoverre de betrokken actoren geen toegang hebben tot de nummerplaatgegevens in het repertorium van de voertuigen (punt 43);
- schrappen van de bepalingen inzake het gebruik van intelligente camera's voor de automatische herkenning van vaartuigen (punten 45 – 46 en 116);
- uitdrukkelijk specifiëren van alle doeleinden waarvoor intelligente camera's desgevallend kunnen worden aangewend (punten 47 – 48);
- schrappen van de onjuistheden in de Memorie van toelichting met betrekking tot een gedoogtermijn van 1 jaar om het gebruik van de biometrische gegevens uit te faseren ofwel om de wetgever aan te sporen te voorzien in een juridisch kader (punt 49);
- specifiëren van alle doeleinden voor de verwerking van biometrische gegevens in artikel 2.5.2.84, §1 (punt 51);
- aanpassen van de formuleringen inzake de vereisten voor een biometrisch systeem (punten 55 – 56);
- specifiëren van een doeleinde voor de verwerking van persoonsgegevens in het kader van de verplichte opleiding en vorming van bepaalde actoren (punten 27 – 28 en 64);
- voorzien in een machtiging voor het gebruik van het Rijksregisternummer in hoofde van de betrokken actoren (punten 70 – 71, 77 en 80);
- schrappen van het informatiegegeven 'identiteitskaart- of paspoortnummer' in artikel 2.5.2.88 (punt 72);
- schrappen van de passage met betrekking tot de toegang tot biometrische gegevens voor de inlichtingendiensten en de federale en lokale politie in artikel 2.5.2.89 (punt 84);

- herwerken van de (maximale) bewaartermijn die geldt ten aanzien van de biometrische gegevens (punten 89 – 90);
- herevalueren van de aanduiding van de PFSO als de verwerkingsverantwoordelijke voor de bezoekers van een havenfaciliteit (punten 94 – 96);
- herwerken van de bepalingen met betrekking tot de inperking van de rechten van de betrokkenen (punten 100 – 103 en 120);
- de voorgestelde wijzigingen/ aanvullingen met betrekking tot de aanvraagprocedure voor het plaatsen van camera's in de Noordzee implementeren (punt 108);
- naar analogie met de Camerawet, bijkomende waarborgen opnemen met betrekking tot het in real time bekijken van beelden (punt 110);
- herwerken van de bepalingen met betrekking tot de vereisten voor het opnemen van beelden en de maximale bewaartermijn van deze beelden (punten 111 – 112);
- wijzigen van artikel 4.6.1.9 met betrekking tot het verbod om heimelijk te filmen zodanig dat het beter overeenstemt met de realiteit (punt 115);
- schrappen van artikel 4.6.1.11 inzake non-discriminatie (punt 118).

Voor het Kenniscentrum,
(get.) Rita Van Nuffelen - Verantwoordelijke a.i. van het Kenniscentrum