PORT PRIVACY

Privacy Gedragscode

Toegangsbeleid ISPS-bedrijven

PORT PRIVACY

Privacy Gedragscode

Toegangsbeleid ISPS-bedrijven

Datum	24 juli 2023
Bedrijf	Port Privacy B.V.
Status	Definitief
Versie	1.0
Auteurs	Tjeerd Poot / Gwynneth Goudsblom

PORT PRIVACY

Intellectueel eigendom en copyright

Het intellectueel eigendom van de Gedragscode ligt louter en alleen bij de besloten vennootschap met beperkte aansprakelijkheid Port Privacy B.V.

PORT PRIVACY

Goedkeuring en inwerkingtreding

De Nederlandse Autoriteit Persoonsgegevens (AP) heeft op XXX een goedkeurende verklaring afgegeven voor de Privacy Gedragscode Toegangsbeleid ISPS-bedrijven (Gedragscode). Deze verklaring is op XXX gepubliceerd in de Staatscourant XXX nr. XXX.

De AP heeft verklaard dat de Gedragscode, gelet op de bijzondere kenmerken van de sector, een juiste uitwerking vormt van de Europese Algemene Verordening Gegevensbescherming (AVG) en andere wettelijke bepalingen die de verwerking van persoonsgegevens betreffen. [deze eventueel tekst aanpassen na ontvangst verklaring]

De goedkeuring geldt voor een periode van XXX jaar.

Deze Gedragscode treedt in werking op de eerstvolgende dag na de hierboven vermelde datum van publicatie van de verklaring van de AP in de Staatscourant.

Het verzoek tot goedkeuring en de verklaring van de AP zijn te vinden in bijlagen 1 en 2. In het verzoek wordt verwezen naar de Guidelines van de European Data Protection Board (EDPB). Een verwijzingstabel is daarom toegevoegd als bijlage 3.

PORT PRIVACY

Inhoudsopgave

1 Inleiding

Dit is de Privacy Gedragscode voor het toegangsbeleid van ISPS-bedrijven in Nederland.

Een ISPS-bedrijf is een havenbedrijf waar internationaal scheepvaartverkeer wordt afgehandeld. Voor een bedrijf waar internationaal scheepvaartverkeer wordt afgehandeld, geldt de verplichting om zich te certificeren voor de International Ship and Port Facility Security Code (ISPS Code). De regelgeving is opgesteld naar aanleiding van de aanslagen op 11 september 2001 en ziet op de veiligheid en beveiliging van schepen en havenfaciliteiten.

Uit de ISPS Code vloeit voort dat ten behoeve van de veiligheid en beveiliging een toegangsbeleid moet worden gevoerd. In de uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Op deze verwerkingen is de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing. Met deze Gedragscode wordt het toegangsbeleid van ISPS-bedrijven in lijn gebracht met de AVG.

De Gedragscode is goedgekeurd door de Nederlandse Autoriteit Persoonsgegevens en staat onder onafhankelijk toezicht. De Gedragscode geldt daarom ook als een verantwoordingsinstrument. Door de Gedragscode te volgen, wordt aangetoond dat aan de AVG wordt voldaan.

Leeswijzer
Na dit inleidende hoofdstuk wordt in de hoofdstukken 2 en 3 omschreven waar de Gedragscode op ziet en wat er mee wordt beoogd. In hoofdstuk 4 wordt toegelicht welke partijen bij de Gedragscode belang hebben. Hoofdstuk 5 ziet op de representativiteit van de Werkgroep. Port Privacy heeft de Gedragscode in samenwerking met deze Werkgroep opgesteld.

In hoofdstuk 6 wordt verantwoording afgelegd. Uit dit hoofdstuk volgt dat een ISPS-bedrijf dat bij de Gedragscode is aangesloten aan de eisen van de AVG voldoet. Aanvullend daarop wordt in hoofdstukken 7 t/m 18 per categorie van betrokkenen (scheepvaartbemanning, werknemers, vrachtautochauffeurs, enz.) beschreven in welke situaties verwerkingen plaatsvinden en om welke persoonsgegevens het gaat.

Voor de praktijk is hoofdstuk 19 het meest relevant. In dat hoofdstuk staan namelijk de gedragsregels. De gedragsregels zijn gedestilleerd uit de hoofdstukken waarin verantwoording is afgelegd. De hoofdstukken 6 t/m 18 vormen dus een toelichting op hoofdstuk 19.

In het laatste hoofdstuk komt het beheer van de Gedragscode en het toezicht op de naleving daarvan aan de orde. In hoofdstuk 20 en in de bijbehorende bijlagen is ook opgenomen aan welke eisen moet worden voldaan om aan de Gedragscode deel te nemen.

Totstandkoming van de Gedragscode
Het proces van totstandkoming van de onderhavige Gedragscode staat beschreven in bijlage 4.

Taal
De Gedragscode is opgesteld in het Nederlands. Dit is de aangewezen taal omdat de Gedragscode ziet op verwerkingen op Nederlands grondgebied door of namens Nederlandse verwerkingsverantwoordelijken en omdat deze taal ook wordt gehanteerd door de bevoegde toezichthoudende autoriteit: de Nederlandse Autoriteit Persoonsgegevens.

Bij onduidelijkheid als gevolg van een eventuele vertaling is de Nederlandse versie van de Gedragscode leidend.

Internationale en nationale wet- en regelgeving
De Gedragscode is in overeenstemming met de toepasselijke internationale (Europese) en nationale wet- en regelgeving. Welke wet- en regelgeving dat betreft, volgt uit de verantwoording van de verwerkingen in hoofdstuk 6.

Definities en afkortingen
Voor een goed begrip van de in de Gedragscode gehanteerde termen en afkortingen wordt verwezen naar de definities die zijn opgenomen in bijlage 5 en naar artikel 4 van de AVG.

PORT PRIVACY

2 Reikwijdte

De Gedragscode ziet op de verwerkingen die plaatsvinden in het kader van het toegangsbeleid van ISPS-bedrijven in Nederland. Dit wordt als volgt toegelicht.

Territoriale reikwijdte: ISPS-bedrijven in Nederland
Een ISPS-bedrijf is een op de internationale handel gericht havengerelateerd bedrijf dat ISPS-gecertificeerd is. Meer informatie hierover is terug te vinden in bijlage 6.

De Gedragscode ziet louter op het toegangsbeleid dat geldt op bedrijfsterreinen op Nederlands grondgebied van Nederlandse vestigingen van ISPS-bedrijven. Het gaat dus om een 'nationale gedragscode'.

Materiële reikwijdte: verwerkingen in het kader van het toegangsbeleid
Elk ISPS-bedrijf voert een beveiligings- en veiligheidsbeleid. Een belangrijk onderdeel daarvan vormt het toegangsbeleid. In de uitvoering van het toegangsbeleid worden o.a. aanmeldingen, aankomsten, verblijfsduur en vertrekmomenten van betrokkenen geregistreerd in een toegangsmanagementsysteem en door camera's. In de uitvoering van het toegangsbeleid worden door of namens ISPS-bedrijven dus persoonsgegevens verwerkt.

De Gedragscode ziet louter op de verwerkingen die plaatsvinden in het kader van het toegangsbeleid. Om welke verwerkingen dit concreet gaat, volgt uit de hoofdstukken 6 t/m 18 waarin verantwoording wordt afgelegd cq. wordt aangetoond dat en hoe aan de eisen van de AVG wordt voldaan.

PORT PRIVACY

3 Doelen

Met de Gedragscode worden de navolgende doelen nagestreefd:

- Het stellen van regels aan ISPS-bedrijven voor het verwerken van persoonsgegevens in het kader van het op veiligheid en beveiliging gerichte toegangsbeleid dat gericht is op:
  - het weten wie er zich op het terrein bevindt en
  - het voorkomen van toegang door onbevoegden.
- Het conformeren van de praktijk van het toegangsbeleid aan de AVG: compliance aan de AVG.
- Het bieden van een effectief verantwoordingsinstrument: toetsbare gedragsregels waardoor compliance aan de AVG kan worden aangetoond.
- Het vastleggen van best practices.
- Het dienen als hulpbron bij het voorkomen en aanpakken van problemen op het gebied van gegevensbescherming.
- Het vergemakkelijken van de toepassing van de AVG.
- Het vergroten van het vertrouwen en de rechtszekerheid in de sector.
- Het bieden van transparantie aan betrokkenen.
- Het verhogen van het gegevensbeschermingsniveau ten behoeve van de betrokkenen.

4 Belanghebbenden

Als belanghebbenden bij de Gedragscode worden onderscheiden:

1 ISPS-bedrijven
2 Havenbeveiligingsbedrijven
3 Beheerders van logistieke informatieplatformen
4 Leveranciers van toegangsmanagementsystemen
5 Leveranciers van camerabeveiligingssystemen
6 Burgemeesters, Colleges van B&W, Havenmeesters en Havenbedrijven
7 Belastingdienst Douane
8 Politie
9 Ondernemersverenigingen
10 Betrokkenen

De genoemde categorieën van belanghebbenden hebben elk een eigen rol. Hieronder komen die rollen aan de orde en wordt duidelijk waarom zij belang hebben bij de Gedragscode. Voor zover relevant komt in hoofdstuk 6 aan de orde welke rol een belanghebbende speelt in het licht van de AVG.

ISPS-bedrijven
ISPS-bedrijven zijn op de internationale handel gerichte bedrijven waar internationaal scheepvaartverkeer wordt afgehandeld. Er zijn 4 subcategorieën onderscheiden: Bulk, Chemische industrie, Containerterminals en Empty depots.

Voor deze havengerelateerde bedrijven is het verplicht om zich te certificeren voor de International Ship and Port Facility Security Code (ISPS Code). De ISPS Code is een amendement op het Verdrag voor beveiliging van mensenlevens op zee (SOLAS) naar aanleiding van de aanslagen op 11 september 2001. De ISPS Code is overgenomen in de Europese verordening 725/2004. Naast de ISPS Code geldt ter nadere uitvoering daarvan, de Havenbeveiligingswet.

De ISPS Code ziet op de veiligheid en beveiliging van schepen en havenfaciliteiten door een vroegtijdige verzameling en uitwisseling van informatie op veiligheidsgebied. Het doel is om burgers en milieu te beschermen tegen het gevaar van opzettelijke ongeoorloofde acties zoals terrorisme, piraterij of vergelijkbare acties zoals drugssmokkel. De ISPS Code zorgt er voor dat dit op een homogene wijze geschiedt. De ISPS Code beoogt voorts een basis te leggen voor een geharmoniseerde interpretatie en implementatie van de communautaire controle op de speciale maatregelen ter verbetering van de veiligheid. Meer in het bijzonder is het doel van de ISPS Code om te zorgen voor een vroegtijdige en doeltreffende verzameling en uitwisseling van informatie op veiligheidsgebied.

ISPS-bedrijven hebben belang bij de Gedragscode omdat daarin de verwerkingen worden verantwoord waar zij verantwoordelijk voor zijn.

Havenbeveiligingsbedrijven
Havenbeveiligingsbedrijven zijn beveiligingsbedrijven met een Nederlandse Dienst-nummer. Dit ND-nummer is gekoppeld aan de vergunning van het Ministerie van Justitie om beveiligingswerkzaamheden te mogen verrichten op basis van de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr).

Havenbeveiligingsbedrijven onderscheiden zich van reguliere beveiligingsbedrijven omdat zij louter werken met beveiligers die in het bezit zijn van een havenbeveiligingscertificaat. Dit is verplicht op grond van artikel 14 van de Havenbeveiligingswet (een uitvoeringswet van de ISPS).

Havenbeveiligingsbedrijven hebben belang bij de Gedragscode omdat zij, als verwerker, de praktische uitvoering moeten geven aan het toegangsbeleid van ISPS-bedrijven.

Beheerders van logistieke informatieplatforms
Beheerders van logistieke informatieplatforms fungeren als digitale spin in het web. Via de platforms wordt informatie, waaronder persoonsgegevens, uitgewisseld tussen schepen, rederijen, agenten, ISPS-bedrijven, leveranciers, enz. De verschillende partijen communiceren zo over de aankomst van een schip, de scheepsbemanning, de leveranciers die het schip moeten bezoeken, enz.

Beheerders hebben belang bij de Gedragscode omdat zij verantwoordelijk zijn voor een belangrijk onderdeel van het toegangsbeleid van ISPS-bedrijven.

Leveranciers van toegangsmanagementsystemen
Leveranciers van toegangsmanagementsystemen onderhouden de door hen geleverde computersystemen waarin kan worden geregistreerd wie zich aanmeldt voor een bezoek, wie zich meldt aan de toegangspoort met een verzoek toegang te krijgen, enz. Bij de toegangsmanagementsystemen worden ook toegangskaarten en uitleesapparatuur geleverd.

Leveranciers hebben belang bij de Gedragscode omdat ze verantwoordelijk zijn voor de levering van, de service aan en het onderhoud van het toegangsmanagementsysteem dat het toegangsbeleid ondersteunt.

Leveranciers van camerabeveiligingssystemen
Leveranciers van camerabeveiligingssystemen hebben belang bij de Gedragscode omdat zij verantwoordelijk zijn voor de service aan en het onderhoud van de door hen geleverde beveiligingscamera's die door ISPS-bedrijven worden gebruikt in het kader van het toegangsbeleid.

Burgemeesters, Colleges van B&W, Havenmeesters en Havenbedrijven
De Havenbeveiligingswet, waarmee uitvoering wordt gegeven aan de ISPS Code, wijst de Burgemeester en het College van B&W aan als bevoegde autoriteit voor de beveiliging van havenfaciliteiten. Zij hebben dus tot taak om toe te zien op de naleving van de ISPS Code door ISPS-bedrijven. In de meeste gemeenten is deze bevoegdheid gedelegeerd aan een Havenmeester cq. een Havenbedrijf. Havenmeesters, havenbedrijven en de achterliggende colleges van B&W hebben grote invloed op het toegangsbeleid van ISPS-bedrijven. Dit heeft bijvoorbeeld geleid tot een toename van de inzet van biometrische verificatie.

Burgemeesters, Colleges van B&W, Havenmeesters en havenbedrijven hebben belang bij de Gedragscode omdat ISPS-bedrijven de ISPS Code naleven door een toegangsbeleid te voeren.

Belastingdienst Douane
De Belastingdienst Douane is de nationaal opererende overheidsinstantie die AEO-vergunningen verleent en toeziet op de naleving daarvan. De AEO-regelgeving is gericht op de veiligheid van de vervoersketen. Bedrijfseconomisch zijn de meeste ISPS-bedrijven genoodzaakt om in het bezit te zijn van een AEO-vergunning. De eisen die uit de AEO voortvloeien, zijn, ter zake van het toegangsbeleid, gelijk aan de eisen die voortvloeien uit de ISPS Code.

De Belastingdienst Douane heeft belang bij de Gedragscode omdat ISPS-bedrijven die een AEO-vergunning hebben, de AEO-eisen naleven door een toegangsbeleid te voeren.

Politie
De politie is een nationaal opererende instantie die gericht is op criminaliteitsbestrijding. Zij heeft belang bij de Gedragscode omdat een toegangsbeleid dat voldoet aan de AVG een beter beheersbare situatie geeft en daarmee criminaliteitsbestrijding ondersteunt.

Ondernemersverenigingen
Een ondernemersvereniging is, in deze Gedragscode, een vereniging die de belangen behartigt van bedrijven die opereren in een internationaal havengebied. Zij hebben belang bij de Gedragscode omdat veel leden van de vereniging vallen onder één van de in dit hoofdstuk beschreven categorieën van belanghebbenden.

Betrokkenen
Betrokkenen zijn de natuurlijke personen die toegang willen tot of zich bevinden op het terrein van een ISPS-bedrijf. Zij hebben belang bij de Gedragscode omdat het gaat om hun persoonsgegevens die in het kader van het toegangsbeleid worden verwerkt. In deze Gedragscode worden verschillende categorieën van betrokkenen onderscheiden (zie hoofdstukken 7 t/m 18):

- Bezoekers
- Binnenvaartbemanning
- Bootmannen en sjorders
- Externe arbeidskrachten
- Kinderen
- Leveranciers en shipchandlers
- Onbevoegd aanwezigen
- Overheidspersoneel
- Scheepsbemanning
- Vrachtautochauffeurs
- Vrachttreinpersoneel
- Werknemers

5 Representativiteit

Een gedragscode dient te zijn opgesteld door een organisatie die representatief is voor de sector van bedrijven waar de gedragscode voor is bedoeld.

Deze Gedragscode is opgesteld door Port Privacy in samenwerking met de Werkgroep. Port Privacy vertegenwoordigt de Werkgroep (zie bijlage 1). De Werkgroep is representatief voor de sector van ISPS-bedrijven. Hieronder volgt een beschrijving van de Werkgroep en wordt voorts ingegaan op de representativiteit.

Werkgroep
De Werkgroep bestaat uit een aantal ISPS-bedrijven en een aantal andere belanghebbenden.

De ISPS-bedrijven die lid zijn van de Werkgroep:
- APM Maasvlakte II B.V.
- APM Terminal Rotterdam B.V.
- European Bulk Services B.V.
- Europees Massagoed Overslagbedrijf B.V.
- Gate Terminal B.V.
- Huntsman Holland B.V.
- Hutchison Ports ECT Rotterdam B.V.
- Kramer Group B.V.
- Rotterdam World Gateway B.V.

Andere belanghebbenden die lid zijn van de Werkgroep:
- Belastingdienst Douane
- by DnA
- Havenbedrijf Rotterdam N.V.
- Royal Dirkzwager B.V.
- Secure Logistics B.V.
- Securitas Rotterdam B.V.
- Vereniging Deltalinqs
- Politie

Representativiteit
De Werkgroep is representatief voor de sector van ISPS-bedrijven. De representativiteit blijkt uit het feit dat alle categorieën van belanghebbenden in de Werkgroep zijn vertegenwoordigd (behalve de betrokkenen): óók alle in de sector relevante overheden zoals het Havenbedrijf Rotterdam, de Belastingdienst Douane en de Politie. Bovendien zijn van de belangrijkste categorie van belanghebbenden, de ISPS-bedrijven, ook de vier onderscheiden subcategorieën in de Werkgroep aanwezig.

Categorie van belanghebbenden	Lid van de werkgroep
• ISPS-bedrijven / Bulk	EMO, EBS
• ISPS-bedrijven / Chemische industrie	Gate, Huntsman
• ISPS-bedrijven / Containerterminals	ECT, APM, APM II, RWG
• ISPS-bedrijven / Empty depots	Kramer
• Havenbeveiligingsbedrijven	Securitas
• Beheerders van logistieke informatieplatforms	Dirkzwager
• Leveranciers van toegangsmanagementsystemen	Secure Logistics
• Havenbedrijven	Havenbedrijf Rotterdam
• Belastingdienst Douane	Belastingdienst Douane Rotterdam
• Politie	Zeehavenpolitie Rotterdam
• Ondernemersverenigingen	Deltalinqs

De representativiteit blijkt voorts uit het feit dat de bedrijventerreinen van de ISPS-bedrijven die lid zijn van de werkgroep, in oppervlakte verreweg het grootste deel van Rotterdamse haven beslaan en (daardoor) ook verantwoordelijk zijn het overgrote deel van de handel die door ISPS-bedrijven wordt gerealiseerd.

Van algemene bekendheid is het feit dat de Rotterdamse haven, de grootste haven in Europa, model staat voor alle andere Nederlandse havens. Dat geldt zeker voor de aldaar gevestigde ISPS-bedrijven.

6 Verantwoording

In dit hoofdstuk worden alle verwerkingen verantwoord: aangetoond wordt dat aan de eisen van de AVG wordt voldaan en hoe dat gebeurt. De verantwoording geschiedt aan de hand van de onderstaande vragen.

Voor de vragen 9 t/m 12 geldt dat het antwoord daarop per categorie van betrokkenen verschillend is. Deze vragen zijn daarom verder uitgewerkt in de hoofdstukken 7 t/m 18.

Vraag 1	Wie is verwerkingsverantwoordelijk?
Vraag 2	Wie is verwerker?
Vraag 3	Zijn er verwerkersovereenkomsten en overeenkomsten t.b.v. gezamenlijke verwerkingsverantwoordelijkheid gesloten?
Vraag 4	Wie is intern verantwoordelijk voor de naleving van de Gedragscode?
Vraag 5	Is er een FG aangesteld?
Vraag 6	Wordt er een verwerkingsregister gevoerd?
Vraag 7	Wat is het doel van de verwerkingen?
Vraag 8	Wat zijn de grondslagen?
Vraag 9	Wie is de betrokkene?
Vraag 10	In welke situaties vinden verwerkingen plaats?
Vraag 11	Om welke verwerkingen gaat het?
Vraag 12	Om welke persoonsgegevens gaat het?
Vraag 13	Worden er bijzondere persoonsgegevens verwerkt?
Vraag 14	Heeft er een DPIA plaatsgevonden voor het camerabeleid?
Vraag 15	Heeft er een DPIA plaatsgevonden voor de inzet van biometrie?
Vraag 16	Hoe worden de persoonsgegevens beveiligd?
Vraag 17	Hoe lang worden de persoonsgegevens bewaard?
Vraag 18	Hoe worden de betrokkenen geïnformeerd?
Vraag 19	Hoe worden de rechten van betrokkenen gewaarborgd?

6.1 Wie is verwerkingsverantwoordelijk?

In alle situaties waarin verwerkingen plaatsvinden in het kader van het toegangsbeleid is het ISPS-bedrijf de verwerkingsverantwoordelijke. Zij hebben immers belang bij en besluiten tot het verwerken van persoonsgegevens. Zij bepalen om welke persoonsgegevens het gaat, van wie de persoonsgegevens worden verwerkt, wat met de persoonsgegevens gebeurt en hoe lang de persoonsgegevens worden bewaard.

6.2 Wie is verwerker?

In alle situaties geldt dat het ISPS-bedrijf een havenbeveiligingsbedrijf heeft ingeschakeld voor het uitvoeren van haar toegangsbeleid en als een verwerker moet worden gekwalificeerd. Het havenbeveiligingsbedrijf verwerkt geen persoonsgegevens zonder de instructie van een ISPS-bedrijf. Zij bepaalt niet om welke gegevens het gaat, met welk doel dit gebeurt en hoe lang de persoonsgegevens worden bewaard

In de situaties waarin gebruik wordt gemaakt van een logistiek informatieplatform om informatie uit te wisselen, is de beheerder van dat platform een verwerker. Het gaat op het moment van schrijven om situaties waarin persoonsgegevens worden verwerkt van de navolgende betrokkenen: bezoekers, bootmannen, sjorders, leveranciers, shipchandlers en scheepsbemanning (zie hoofdstukken 7, 9, 12 en 15).

In de situatie dat er service of onderhoud aan het toegangsmanagementsysteem plaatsvindt, is de leverancier van het toegangsmanagementsysteem een verwerker.

In de situatie dat er service of onderhoud aan het camerabeveiligingssysteem plaatsvindt, is de leverancier van het camerabeveiligingssysteem een verwerker.

6.3 Zijn er verwerkersovereenkomsten en overeenkomsten t.b.v. gezamenlijke verwerkingsverantwoordelijkheid gesloten?

Ja. Elk ISPS-bedrijf heeft verwerkersovereenkomsten gesloten met de verwerkers die op haar instructie persoonsgegevens verwerken in het kader van het toegangsbeleid. In deze verwerkersovereenkomsten is expliciet opgenomen dat de verwerker is gehouden om, net als het ISPS-bedrijf, de Gedragscode te volgen. Voorts zijn er overeenkomsten gesloten met betrekking tot de gezamenlijke verwerkingsverantwoordelijkheid (zie ‘Wie is verwerkingsverantwoordelijk?’). Daarin zijn afspraken vastgelegd over wie waarvoor verantwoordelijk is.

6.4 Wie is er intern verantwoordelijk voor de naleving van de Gedragscode?

Het ISPS-bedrijf belast ten minste één medewerker met de verantwoordelijkheid voor de naleving van de Gedragscode. De naam en de contactgegevens van deze medewerker worden genoemd in de privacyverklaringen.

6.5 Is er een FG aangesteld?

Het is aan ISPS-bedrijven zelf om te bepalen of een FG wordt aangesteld. Wordt geen FG aangesteld dan worden de overwegingen om dat na te laten, opgenomen in het interne privacybeleid.

Relevant voor het maken van een keuze is met name artikel 37 AVG waarin staat dat het verplicht is een FG aan te stellen indien een verwerkingsverantwoordelijke hoofdzakelijk belast is met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen. De AP zegt daarover op haar website dat het aanstellen van een FG verplicht is voor organisaties die ‘vanuit hun kernactiviteiten op grote schaal individuen volgen of diens activiteiten in kaart brengen. Het kan dan bijvoorbeeld gaan om cameratoezicht. Relevant is onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang mensen worden gevolgd.’

6.6 Wordt er een verwerkingsregister gevoerd?

Elk ISPS-bedrijf voert een verwerkingsregister. In het verwerkingsregister worden geregistreerd:

- Identiteit en contactinformatie van het ISPS-bedrijf en van de FG of privacy officer.
- De doelen van de verwerkingen (zie paragraaf 6.7).
- De categorieën betrokkenen (zie hoofdstuk 7 t/m 18).
- De categorieën van persoonsgegevens (zie hoofdstuk 7 t/m 18).
- De categorieën van interne ontvangers (binnen de organisatie van het ISPS-bedrijf).
- De categorieën van eventuele externe ontvangers in de EU.
- De categorieën van eventuele externe ontvangers buiten de EU.
- De eventuele doorgiften aan 3e landen (met verwijzing naar waarborgen).
- De bewaartermijn (zie paragraaf 6.17).
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

6.7 Wat is het doel van de verwerkingen?

Alle verwerkingen worden verricht in het kader van het toegangsbeleid. Het toegangsbeleid is onderdeel van het beveiligings- en veiligheidsbeleid van een ISPS-bedrijf en gebaseerd op (met name) de ISPS Code.

Het is voor een ISPS-bedrijf o.a. uit hoofde van de ISPS Code verplicht om er mee bekend te zijn wie er zich op het terrein bevindt en om te voorkomen dat onbevoegden zich toegang verschaffen. In dat kader dient niemand op het terrein te worden toegelaten zonder controle van de identiteit en controle op de reden om toegang te willen verkrijgen. Het doel van de verwerkingen is dus telkens gericht op beveiliging en veiligheid in het algemeen en op de controle van de identiteit en de reden om toegang te willen verkrijgen, in het bijzonder.

Voorts is een ISPS-bedrijf o.a. uit hoofde van de Arbeidsomstandighedenwet gehouden om een volledige registratie te voeren van de aanwezigen op het terrein, zodat er, wanneer nodig, een volledige ontruiming kan plaatsvinden. Betrokkenen kunnen hierdoor op een veilige en

verantwoorde wijze uit een eventuele gevarenzone worden weg geleid. Deze registratie vormt onderdeel van het toegangsbeleid.

Het toegangsbeleid is tot slot noodzakelijk om het bedrijfseconomische en commerciële proces van ISPS-bedrijven efficiënt en effectief te laten verlopen.

6.8 Wat zijn de grondslagen?

Alle verwerkingen zijn gerechtvaardigd omdat ze noodzakelijk zijn voor het behartigen van de gerechtvaardigde belangen van ISPS-bedrijven of derden. Hieronder wordt deze grondslag ex artikel 6 lid 1 sub f AVG nader uitgewerkt aan de hand van de drie voor die grondslag geldende voorwaarden en conform de Normuitleg van de AP.

De eerste voorwaarde: zijn de belangen gerechtvaardigd?
De Normuitleg van de AP luidt op dit punt: '*De eerste voorwaarde is dat de belangen van de verwerkingsverantwoordelijke of een derde kwalificeren als gerechtvaardigd. Dat houdt in dat die belangen in (algemene) wetgeving of elders in het recht zijn benoemd als een rechtsbelang. Een belang dat ook in rechte beschermd wordt, dat beschermingswaardig wordt geacht en dat in beginsel gerespecteerd moet worden en 'afgedwongen' kan worden.'*

De belangen van ISPS-bedrijven die het verwerken van persoonsgegevens in het kader van het toegangsbeleid noodzakelijk maken, betreffen: het belang van beveiliging, het belang van veiligheid en het (sub)belang van de bedrijfscontinuïteit. Opgemerkt wordt dat laatstgenoemd belang in delen uiteen valt en dat één daarvan wederom het veiligheidsbelang betreft. De belangen en de rechtvaardiging daarvan worden hieronder toegelicht.

Het belang van beveiliging en het belang van veiligheid
Het belang van beveiliging ziet op het voorkomen van criminaliteit en terreurdaden. Van algemene bekendheid is dat de Nederlandse zeehavens relatief vaak worden geconfronteerd met criminele activiteiten, zoals drugssmokkel, mensensmokkel en ladingdiefstal.

Het belang van veiligheid ziet op het voorkomen van ongelukken, incidenten, rampen, enz. die een bedreiging vormen voor de gezondheid van personeel en de volksgezondheid van de mensen in de nabije en verre omgeving van het havengebied.

Het mag duidelijk zijn dat het hier niet gaat om speculatieve, toekomstige, maar om echte, concrete en rechtstreekse belangen. De bovenstaande belangen komen in diverse wet- en regelgeving naar voren als een rechtsbelang; als een belang dat beschermingswaardig wordt geacht en dat in beginsel gerespecteerd moet worden en 'afgedwongen' kan worden. Verwezen wordt naar onderstaand overzicht, de onderstaande toelichting daarop en de bijlagen 7 t/m 12.

Arbeidsomstandighedenwet	3 lid 1 sub e, 6, 10 en 15
AEO-regelgeving (titel 1, afdeling 4)	39 sub e
BRZO	5 lid 1 en 2
Havenbeheersverordening	11.2.2 lid 2 en 3, 11.2.3 sub e, 11.4.2 sub d en 11.4.3 lid 3 en 4
ISPS Code (Bijlage II, Deel A)	14 lid 2, 16 lid 3 sub 2 en 17 lid 2 sub 8
ISPS Code (Bijlage III, Deel B)	16 lid 13 t/m 15 en 16 lid 17

In de genoemde bijlagen staan de wetsartikelen uitgeschreven. Vervolgens wordt uitgelegd waarom de wetsartikelen de verwerkingen rechtvaardig en noodzakelijk maken. In het kort komt het er op neer dat de arbeidsomstandighedenwet een veilige werkvloer eist, dat de AEO een

veilige vervoersketen eist en dat de ISPS Code, de Havenbeveiligingswet, de BRZO en de Havenbeheersverordening een veilig en beveiligd terrein eisen. Deze wetten noodzaken tot een veiligheids- en beveiligingsbeleid en dus tot een toegangsbeleid en dus tot het verwerken van persoonsgegevens.

Het belang van bedrijfscontinuïteit (cruciaal voor veiligheid)

Het is goed om het belang van bedrijfscontinuïteit separaat te benoemen. Het belang valt in drie delen uiteen: het belang van bedrijfscontinuïteit is cruciaal voor de veiligheid, het dient (logischerwijs) het bedrijfsbelang en tot slot dient het de belangen van derden. Voor de goede orde: het belang van bedrijfscontinuïteit betreft dus niet een ‘zuiver commercieel belang’ zoals bedoeld in de Normuitleg van de AP. Ter toelichting geldt het volgende.

Een stagnerend toegangsbeleid leidt tot onwenselijke en zelfs maatschappij ontwrichtende situaties. Loopt het toegangsbeleid niet soepel dan heeft dat maatschappelijke (veiligheids)consequenties; die overigens veel concreter zijn dan het begrip ‘het algemeen belang’ waarnaar wordt gerefereerd in de Normuitleg.

Er ontstaan bijvoorbeeld gevaarlijke verkeersopstoppingen met gestrande chauffeurs. Een ISPS-bedrijf zoals bijvoorbeeld RWG heeft *per dag* te maken met circa 6.000 vrachtauto’s; en dat gaat dus om nog maar één ISPS-bedrijf! Zouden die vrachtauto’s stranden en dus een file vormen, dan is de chaos na enkele uren, laat staan dagen, niet meer te overzien. Behalve tot files op de weg en daardoor hulpbehoevende chauffeurs leidt een stagnerend toegangsbeleid dan ook tot een chaotische, onhygiënische en risicovolle opstapeling van containers en bulkgoederen, chemische- en andere grondstoffen op de terreinen en tot aanzuigende, groeiende (drugs)criminaliteit. Voedsel gaat rotten, productieprocessen blijven verstoken van grondstoffen en belangrijke onderdelen. Het risico op ongelukken/incidenten neemt toe. Fabrieken vallen stil en kunnen op hun beurt niet leveren. Toeleveranciers worden niet meer ingeschakeld. Mensen verliezen hun baan, enzovoorts.

Het belang van bedrijfscontinuïteit is dus cruciaal voor de veiligheid en de belangen van derden: de duizenden bedrijven en daarmee gezinnen die afhankelijk zijn van een soepel lopende haveneconomie en vervoersketen: en daarmee van de gehele maatschappij. Niet voor niets wordt de haven vaak de motor van de economie genoemd: die moet blijven draaien. Het gaat dan om de talloze mensen die hun inkomen genereren met werkzaamheden die gerelateerd zijn aan de werkzaamheden in de haven en vervoersketen.

Tot slot ten aanzien van de eerste voorwaarde

Ook uit het feit dat de Nederlandse zeehavens als ‘vitale sector’ zijn gekwalificeerd volgt dat ISPS-bedrijven een gerechtvaardigd belang hebben bij de verwerkingen die plaatsvinden in het kader van het toegangsbeleid (zie bijlage 13).

Tot slot geldt dat de beschreven belangen nauw aansluiten bij de voorbeelden uit de Normuitleg: een veilig en gezond leven (incident/ramp), het beschermen van eigendommen / inbreuken op persoonlijkheids- of vermogensrecht tegengaan (diefstal), het onderbouwen van een rechtsvordering (aansprakelijkheidszaak na schade aan container), onrechtmatig gedrag tegengaan (drugshandel), zorgplichten nakomen voor werknemers en/of klanten (veilige

werkvloer), ‘aan alle verplichtingen voldoen die op een bedrijf rust op basis van bijvoorbeeld het Burgerlijk Wetboek (boek 7)’ en ‘zich gedragen overeenkomstig hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt’ (het voorkomen van rampen, criminaliteit, drugshandel, onveilige situaties, overlast, enz.).

Kortom, de belangen zijn gerechtvaardigd. Ze vereisen een algemeen beveiligings- en veiligheidsbeleid met als cruciaal onderdeel daarvan: een betrouwbaar en sluitend toegangsbeleid. Het voeren van een gedegen toegangsbeleid sluit niet voor niets naadloos aan bij de op beveiliging en veiligheid gerichte regelgeving die is ontstaan na de terreuraanslagen van 9/11, zoals de ISPS. Het is noodzakelijk om als ISPS-bedrijf te weten wie er wanneer en om welke reden op het terrein aanwezig is of was.

De tweede voorwaarde: zijn de verwerkingen noodzakelijk?
De Normuitleg van de AP luidt op dit punt: ‘*Kwalificeert het belang zich als gerechtvaardigd? Dan beoordeelt de verwerkingsverantwoordelijke of derde vervolgens of de verwerking van de persoonsgegevens in deze concrete situatie noodzakelijk is om dat belang te behartigen. Daarbij toetst de verwerkingsverantwoordelijke of derde ook of aan de eisen van proportionaliteit en subsidiariteit is voldaan. Dat houdt in: staat de inbreuk voor betrokkene in verhouding tot het doel van de gegevensverwerking? En is het doel niet op een andere manier te bereiken, die minder nadelig is voor de betrokkene?’* Deze vragen worden hieronder beantwoord.

Staat de inbreuk voor betrokkenen in verhouding tot het doel van de gegevensverwerking?
Ja. De inbreuk die de onderhavige verwerkingen voor de betrokkenen oplevert, staat in verhouding tot de doelen van de verwerkingen die zijn omschreven in paragraaf 6.7.

Kort gezegd zijn de verwerkingen gericht op de beveiliging en veiligheid in het algemeen en op de controle van de identiteit en de reden om toegang te willen verkrijgen, in het bijzonder: zodat men weet wie er zich op terrein bevindt bijvoorbeeld voor het geval er zich calamiteiten voordoen en er moet worden ontruimd.

De verwerkingen zijn noodzakelijk om de beschreven gerechtvaardigde belangen te dienen. Immers, zonder die verwerkingen, oftewel zonder een goed georganiseerd toegangsbeleid, kunnen die belangen niet worden gediend. Voor een veilige werkvloer waarop ongelukken, rampen en drugscriminaliteit zoveel mogelijk worden bestreden, is het noodzakelijk om een gedegen toegangsbeleid te voeren en daar zijn alle in de Gedragscode opgenomen verwerkingen voor nodig.

In een voorbeeld: als een bezoeker (hoofdstuk 7) toegang wil tot het terrein, houdt hij zijn toegangskaart tegen een uitleesapparaat dat verbonden is met het systeem. Het systeem vergelijkt de gegevens en als het overeenkomt, dan wordt er toegang verleend en dat wordt dan geregistreerd. De verwerkingen van persoonsgegevens die in dat geval plaatsvinden, zijn noodzakelijk. Immers, door het vergelijken wordt duidelijk om wie het gaat en door de aanwezigheid te registreren, kan hij of zij worden gered als er zich een ramp voltrekt (of kan worden nagegaan of hij of zij met een bepaalde drugssmokkel of schade-

aansprakelijkheidszaak te maken kan hebben, enz. enz.). De met de verwerking gepaard gaande inbreuk op de privacy van de betrokkenen staat in (de juiste) verhouding tot het doel dat bovendien niet op een andere, minder nadelige manier is te bereiken. Nogmaals: voor een goed veiligheid/toegangsbeleid is het noodzakelijk dat bekend is wie er op het terrein is.

Het feit dat daar persoonsgegevens voor moeten worden verwerkt, is dus ook in het belang van de betrokkenen zelf. Daarbij geldt dat de inbreuk die plaatsvindt, beperkt is; te meer nu er diverse maatregelen worden genomen om de inbreuk zo klein mogelijk te laten zijn en de nadelige gevolgen zo klein mogelijk (zie o.a. paragraaf 6.12 en 6.16).

Is het doel niet op een andere manier te bereiken, die minder nadelig is voor de betrokkenen?
Nee. Er zijn geen realistische alternatieven. Uiteraard wordt het toegangsbeleid zo ingericht dat het zo min mogelijk inbreuk of nadeel oplevert voor de betrokkenen. Daar is de Gedragscode op gericht. Er is geen manier bekend waarop het kan worden ingericht waardoor het nog minder nadelig zou worden.

Het verwerken van minder persoonsgegevens leidt tot veiligheidsrisico's: door minder persoonsgegevens te verwerken, is het niet mogelijk om (in voldoende mate en gedurende een benodigde periode) te weten wie er op het terrein is en of die daartoe bevoegd is. Om de doelen te bereiken en de belangen te behartigen, is de verwerking nodig van alle opgesomde persoonsgegevens. Het korter bewaren van de persoonsgegevens is eveneens niet wenselijk. Verwezen wordt naar paragraaf 6.17 (bewaartermijn). Ook het invoeren van willekeurige controles volstaat niet. Dit zou leiden tot chaos en onveilige situaties. De toegangscontrole is er immers o.a. op gericht om te weten wie er op het terrein aanwezig zijn voor het geval er bijvoorbeeld ontruimd moet worden. Bij willekeurige controles is dat niet mogelijk.

Tot slot ten aanzien van de tweede voorwaarde
Uit het voorgaande volgt dat de verwerkingen noodzakelijk zijn.

De derde voorwaarde: Wat is het resultaat van de belangenafweging?
De Normuitleg van de AP luidt op dit punt: *'Vervolgens vindt als derde, cumulatieve voorwaarde een afweging plaats tussen de belangen van de verwerkingsverantwoordelijke of derde enerzijds en de belangen van de betrokkene anderzijds. Bij die afweging betrekt de verwerkingsverantwoordelijke of derde onder meer de volgende factoren:*

- *de gevolgen voor de betrokkene;*
- *de (aanvullende) waarborgen die de verwerkingsverantwoordelijke of derde heeft getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of beperken;*
- *de ernst van de inmenging op het grondrecht van de betrokkene;*
- *of de betrokkene de verwerking min of meer kan verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor diegene toestemming heeft gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.*

Hieronder wordt aan de hand van deze factoren uitgelegd dat de belangen van de ISPS-bedrijven zwaarder wegen dan die van de betrokkenen.

PORT PRIVACY

Wat zijn de gevolgen voor de betrokkene?
De gevolgen van de verwerkingen zijn voor de betrokkenen zeer beperkt. De verwerkingen in het kader van het toegangsbeleid zouden een gevoel kunnen geven van minder bewegingsvrijheid, maar feitelijk gaat het niet om ernstige inmenging op grondrechten, zoals het grondrecht van bewegingsvrijheid; terwijl daar verhoogde veiligheid tegenover staat.

Een betrokkene merkt er feitelijk niks van (anders dan dat hij of zij toegang krijgt tot een, mede door het toegangsbeleid bewerkstelligde, veilig en beveiligd terrein). Immers:

- de persoonsgegevens worden louter gebruikt voor het doel: het toegangsbeleid ('wie is er wanneer') (paragraaf 6.7),
- de gegevens worden beveiligd (paragraaf 6.16) en
- niet langer dan de gerechtvaardigde bewaartermijn bewaard (paragraaf 6.17),
- de betrokkenen worden geïnformeerd (paragraaf 6.18) en
- de rechten van betrokkenen worden gewaarborgd (paragraaf 6.19).

Wat zijn de (aanvullende) waarborgen die de verwerkingsverantwoordelijke of derde heeft getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of beperken?
In antwoord op deze vraag wordt verwezen naar al hetgeen hierover blijkt in Hoofdstuk 6. Zo worden er uiteraard niet meer persoonsgegevens verwerkt dan noodzakelijk is om het doel van de verwerking te bereiken (zie paragraaf 6.12), worden de persoonsgegevens beveiligd (zie paragraaf 6.16) en worden persoonsgegevens niet langer bewaard dan noodzakelijk (paragraaf 6.17).

Wat is de ernst van de inmenging op het grondrecht van de betrokkene?
Het gaat, vooral gezien de gevolgen voor de betrokkenen, om een niet-ernstige inmenging op de grondrechten van betrokkenen, te weten het grondrecht op privacy (bescherming persoonlijke levenssfeer, bescherming tegen ongeoorloofd gebruik van persoonsgegevens) en het grondrecht op bewegingsvrijheid.

Kan de betrokkene de verwerking min of meer kan verwachten?
Ja. Het is, zeker binnen de in deze Gedragscode opgenomen categorieën van betrokkenen, van algemene bekendheid dat ISPS-bedrijven een beveiligings- en veiligheidsbeleid en dus een toegangsbeleid (moeten!) voeren en voorts dat dit betekent dat er persoonsgegevens moeten worden verwerkt.

Tot slot ten aanzien van de derde voorwaarde (belangenafweging)
Gezien de beschreven gerechtvaardigde belangen en de antwoorden op bovenstaande vragen conform de Normuitleg en alle feiten en omstandigheden die in de afgelopen jaren naar voren zijn gekomen uit het werkveld, de media en bijvoorbeeld het EUR-onderzoeksrapport over de criminaliteit in de Rotterdamse haven, wegen de belangen van de verwerkingsverantwoordelijken zwaarder dan die van de betrokkenen.

Dit is de conclusie van de belangenafweging waarvoor ter illustratie een diagram is opgesteld in bijlage 14. Het diagram geeft per potentiële gebeurtenis het risico weer: de kans dat het gebeurt (groot of klein) en de impact ervan als het gebeurt (groot of klein).

De conclusie is duidelijk: het belang van een ‘inbreuk op de privacy makend en op de veiligheid gericht toegangsbeleid’ weegt zwaarder dan een ‘de privacy volledig respecterend cq. non-existent toegangsbeleid’.

Conclusie: aan alle voorwaarden wordt voldaan
Uit het voorgaande volgt dat aan alle voorwaarden wordt voldaan en de verwerkingen dus kunnen worden gegrond op het gerechtvaardigd belang zoals bedoeld in artikel 6 lid 1 sub f AVG.

6.9 Wie zijn de betrokkenen?

In de gedragscode worden meerdere categorieën van betrokkenen onderscheiden. Het gaat om:

- Bezoekers (zie hoofdstuk 7)
- Binnenvaartbemanning (zie hoofdstuk 8)
- Bootmannen en sjorders (zie hoofdstuk 9)
- Externe arbeidskrachten (zie hoofdstuk 10)
- Kinderen (zie hoofdstuk 11)
- Leveranciers en shipchandlers (zie hoofdstuk 12)
- Onbevoegd aanwezigen (zie hoofdstuk 13)
- Overheidspersoneel (zie hoofdstuk 14)
- Scheepsbemanning (zie hoofdstuk 15)
- Vrachtautochauffeurs (zie hoofdstuk 16)
- Vrachttreinpersoneel (zie hoofdstuk 17)
- Werknemers (zie hoofdstuk 18)

6.10 In welke situaties vinden verwerkingen plaats?

Dit verschilt per categorie van betrokkenen. Verwezen wordt naar het betreffende hoofdstuk (zie hoofdstukken 7 t/m 18).

6.11 Om welke verwerkingen gaat het?

Dit verschilt per categorie van betrokkenen en per situatie. Verwezen wordt naar het betreffende hoofdstuk (zie hoofdstukken 7 t/m 18).

6.12 Om welke persoonsgegevens gaat het?

Dit verschilt per categorie van betrokkenen. Verwezen wordt naar het betreffende hoofdstuk (zie hoofdstukken 7 t/m 18). Uiteraard worden er alleen persoonsgegevens verwerkt indien dit noodzakelijk is om het doel van de verwerking te bereiken.

6.13 Worden er bijzondere persoonsgegevens verwerkt?

In beginsel is het antwoord op deze vraag: nee. Het verwerken van bijzondere persoonsgegevens is immers alleen bij uitzondering toegestaan. Worden er in het kader van het

toegangsbeleid toch bijzondere persoonsgegevens verwerkt dan is er sprake van zo'n uitzondering en betreffen het telkens 'biometrische gegevens met het oog op unieke identificatie'.

Biometrische gegevens met het oog op unieke identificatie (zie ook bijlage 15)

Algemeen

Biometrische persoonsgegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

Let op: in deze Gedragscode wordt (vooral) gesproken over de vingerscan. Dat wat daarover staat vermeld, geldt ook voor een handscan of oogscan. Komen er in de toekomst meer vormen bij dan zal de Gedragscode daar op worden aangepast.

Het verwerken van biometrische gegevens met het oog op de unieke identificatie van een persoon is verboden. Op dit verbod is een uitzondering gemaakt in artikel 29 UAVG. Het verbod is niet van toepassing indien (ten eerste) de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Daarbij geldt (ten tweede) dat er voorts sprake moet zijn van een zwaarwegend belang zoals bedoeld in de MvT bij art. 29 UAVG. Er is dus sprake van een dubbele noodzakelijkheidstoets.

De dubbele noodzakelijkheidstoets voor ISPS-bedrijven

Biometrische verificatie in het kader van het toegangsbeleid van een ISPS-bedrijf gebeurt om te kunnen vaststellen dat degene is wie hij stelt te zijn (authenticatie) en om te voorkomen dat toegang wordt verleend aan onbevoegden (beveiliging) én (dus) omwille van de veiligheid: een zwaarwegend algemeen belang.

Het is aan het ISPS-bedrijf zelf om voorafgaand aan de inzet van biometrie een DPIA te verrichten en om gemotiveerd aan de dubbele noodzakelijkheidstoets te voldoen, en aldus om te motiveren dat er sprake is van een zwaarwegend algemeen belang.

Hieronder volgen enkele overwegingen/factoren die een ISPS-bedrijf in haar besluitvorming kan meenemen.

- Bemerkt het ISPS-bedrijf dat haar medewerkers worden geronseld door de georganiseerde criminaliteit om de toegangskaart af te geven (door omkoping, chantage, intimidatie en/of bedreiging), dan is dat een factor die meeweegt bij de vraag of biometrie wordt ingezet. Het gebruik van biometrische verificatie brengt het beveiligingsniveau naar een hoger niveau. Het zorgt er voor dat een ISPS-bedrijf er nagenoeg volledig zeker van kan zijn dat degene die de toegangskaart en het aderpatroon van diens vinger aanbiedt, bevoegd is om zich toegang tot het terrein te verschaffen. Onbevoegde toegang en identiteitsfraude wordt voorkomen.

- Verwerkt een ISPS-bedrijf goederen of stoffen die een target vormen voor (drugs)criminelen en/of terroristen, dan is dat een factor die meeweegt bij de vraag of biometrie wordt ingezet. Voorkomen moet immers worden dat drugs gemakkelijk kan worden verborgen tussen andere lading (zoals vaak bij fruithandel gebeurt) of giftige stoffen worden ingezet bij een terroristische aanslag.

- Verwerkt een ISPS-bedrijf goederen of stoffen waarbij de impact groot is in het geval daarmee een veiligheidsincident plaatsvindt, zoals dat bijvoorbeeld het geval is bij BRZO-bedrijven, is dat een factor die meeweegt om biometrie in te zetten.

- Het gebruik van biometrische verificatie zorgt er voor dat het bedrijfsproces veel efficiënter verloopt. Dit is cruciaal voor de veiligheid. Het proces aan de poort waarbij een betrokkene zich moet identificeren geschiedt vele malen sneller en trefzekerder. Het voorkomt daardoor lange files aan de toegangspoorten en stagnatie van de Nederlandse haveneconomie en vervoersketen. Verwezen wordt naar paragraaf 6.8. In het geval dit risico wezenlijk aanwezig is bij het ISPS-bedrijf dan is dit een factor die meeweegt bij de vraag of biometrie kan worden ingezet.

- Het gebruik van biometrische verificatie zorgt voor een vermindering van het aantal beveiligers dat bij het toegangsproces is betrokken. Een betrokkene hoeft zich minder vaak te legitimeren. De kans op het maken van menselijke fouten neemt af. Is dit risico op privacy-incidenten bij een ISPS-bedrijf in hoge mate aanwezig dan is dit een factor die meeweegt bij de vraag of biometrie wordt ingezet.

Betrokkenen hebben keuzevrijheid

Een betrokkene kan er altijd voor kiezen om toegang tot het ISPS-bedrijf te verzoeken zonder verwerking van biometrische gegevens. Daar zitten voor de betrokkene geen nadelen aan vast, anders dan dat de procedure langer kan duren. Betrokkene dient in dat geval immers te parkeren, uit te stappen, naar de beveiligersloge te lopen, zich te laten legitimeren door een havenbeveiliger, terug te lopen, in te stappen om vervolgens op te rijden naar de toegangspoort alwaar de slagboom omhoog wordt gezet door een havenbeveiliger; terwijl een betrokkene bij gebruikmaking van biometrische verificatie direct kan oprijden naar de scan aan de toegangspoort en de slagboom vervolgens automatisch omhoog gaat).

6.14 Heeft er een DPIA plaatsgevonden op het camerabeleid?

Elk ISPS-bedrijf maakt in de uitvoering van haar toegangsbeleid gebruik van camera's en voert in dat kader een camerabeleid (cameraprotocol). Elk ISPS-bedrijf heeft op het camerabeleid een DPIA uitgevoerd; zoals dat verplicht is gesteld door de AP.

Conform de Beleidsregels Cameratoezicht van de AP d.d. 28 januari 2016 zijn in de DPIA en in het camerabeleid, de relevante vragen gesteld en, mede aan de hand van de Gedragscode, beantwoord. Hieronder volgen de vragen en de (verkort weergegeven) antwoorden.

Wat is het doel?
Het monitoren van bedrijfsprocessen en goederen/stoffen & het beveiligen van personen, gebouwen en goederen/stoffen; o.a. door de toegang door onbevoegden te voorkomen (zie ook paragraaf 6.7).

Wat is de grondslag?
Zie paragraaf 6.8.

Is de inzet noodzakelijk?
De inzet is proportioneel en subsidiair. Het camerabeleid is een noodzakelijke aanvulling op alle andere beveiligingsmaatregelen.

Wat wordt met de beelden gedaan?
Zie paragraaf 6.7 en 6.17.

Hoe worden betrokkenen geïnformeerd?
Zie paragraaf 6.18.

Is eventuele verwerking van bijzondere persoonsgegevens bezwaarlijk?
Uit de DPIA volgt telkens dat het, gezien de doelen, niet op bezwaren stuit dat er bij het gebruik van camera's mogelijk bijzondere persoonsgegevens worden verwerkt omdat:

- Het doel niet is het verwerken van bijzondere persoonsgegevens.
- Het doel niet is het maken van onderscheid aan de hand van bijzondere persoonsgegevens.
- Het in redelijkheid niet is te voorzien dat een dergelijk onderscheid zal worden gemaakt.
- Het doel niet is om betrokkenen te identificeren.
- De inzet van camera's onvermijdelijk is om de doelen te bereiken.

6.15 Heeft er een DPIA plaatsgevonden op de inzet van biometrie?

Elk ISPS-bedrijf dat gebruik maakt van biometrische verificatie heeft daarvoor een leverancier van een toegangsmanagementsysteem ingeschakeld die voldoet aan de ISO-norm 27001 voor informatiebeveiliging.

Deze leverancier heeft op dit deel van haar dienstverlening een DPIA verricht; zoals dat verplicht is gesteld door de AP. Evenwel zal elk ISPS-bedrijf dat gebruik maakt van biometrische verificatie ook zelf een DPIA moeten verrichten.

6.16 Hoe worden de persoonsgegevens beveiligd?

ISPS-bedrijven nemen in het kader van hun privacybeleid veel passende, technische en organisatorische beveiligingsmaatregelen en maken in ieder geval gebruik van:

- Data encryptie
- Data back up
- Opslag van data bij een secured data center
- Offsite data back up
- Network port security
- Network authentication
- Network segmentation
- Antivirus en antimalware
- Firewalling
- Role based access control
- Logging

Voorts geldt in ieder geval het volgende:

- Het ISPS-bedrijf voldoet aan de eisen van de ISO-norm 27001 voor informatiebeveiliging en de ISO-norm 27701 voor privacy.
- Het ISPS-bedrijf maakt alleen gebruik van leveranciers van toegangsmanagementsystemen die voldoen aan de eisen van de ISO-norm 27001 voor informatiebeveiliging.
- Alle digitale bestanden en systemen waarin persoonsgegevens zijn opgeslagen, worden beveiligd met een wachtwoord. Er wordt multifactorauthenticatie toegepast.
- Wachtwoorden zijn alleen bekend bij de personen die de gegevens nodig hebben om hun functie en de daar bijbehorende taken goed uit te kunnen voeren.
- Wachtwoorden worden periodiek gewijzigd.
- Digitale systemen worden periodiek gecontroleerd op virussen en andere onregelmatigheden.
- Digitale systemen worden voortdurend geüpdatet met de nieuwste versie van de betreffende software.
- Digitale systemen draaien op servers die in de Europese Economische Ruimte (EER) staan zodat persoonsgegevens niet daarbuiten worden opgeslagen.
- Havenbeveiligers worden elke 3 jaar gescreend door het Ministerie van Justitie (Justis).
- ISPS-bedrijven hanteren een protocol aan de hand waarvan wordt bepaald of en wanneer het datalek wordt gemeld aan de AP en/of aan betrokkenen (zie bijlage 16).
- Wordt gebruik gemaakt van biometrische verificatie dan wordt het biometrische template enkel opgeslagen op de toegangskaart en niet in de centrale systemen.

6.17 Hoe lang worden de persoonsgegevens bewaard?

Voor alle persoonsgegevens die in het kader van het toegangsbeleid worden verwerkt, ook voor camerabeelden, geldt een bewaartermijn van maximaal 1 jaar. Dit geldt slechts niet voor de persoonsgegevens van kinderen; die worden uit het toegangsmanagementsysteem verwijderd zodra het kind aan of van boord is van het binnenvaartschip (zie hoofdstuk 8).

De termijn van 1 jaar is gerechtvaardigd omdat dit het belang dient van beveiliging, veiligheid en bedrijfscontinuïteit (cruciaal voor de veiligheid). Ter toelichting geldt hetgeen is opgenomen in paragraaf 6.8 en het navolgende.

Wanneer er sprake is van (drugs)criminaliteit, mensensmokkel of ladingdiefstal of wanneer er sprake is van ongelukken, incidenten of rampen, dan is het noodzakelijk om onderzoek te doen zodat kan worden achterhaald wat er is gebeurd en hoe het in de toekomst kan worden voorkomen en wie er eventueel aansprakelijk gesteld of vervolgd kan worden. Dat onderzoek geschiedt alleen effectief en efficiënt als er persoonsgegevens zijn bewaard. Zodoende heeft de bewaartermijn ook een preventieve, afschrikwekkende functie.

De bewaartermijn is voorts van belang van de veiligheid om, in het geval van een incident met gevaarlijke stoffen, ook lang na dat incident, contact te kunnen opnemen met de mensen die bij het incident aanwezig waren omdat het effect van een dergelijk incident zich pas later kan uiten (vergelijk het, louter ter begrip, met een longziekte als gevolg van het werken met asbest 20 jaar eerder).

Voorts wordt de bewaartermijn gehanteerd omdat het daarmee mogelijk blijft om het bedrijfseconomische, commerciële en financiële proces efficiënt en effectief af te ronden. Een lading (bijvoorbeeld een container) reist bijvoorbeeld van A naar B. Die reis kan lang duren. Reizen van een jaar zijn geen uitzondering. Ergens gedurende de reis is een lading korte tijd aanwezig op het terrein van een ISPS-bedrijf. Gedurende de reis kan de lading beschadigd raken. Een schadeclaim kan gedurende de reis worden ingediend, maar wordt logischerwijs meestal ingediend na afloop van de reis. Ontvangt een ISPS-bedrijf een schadeclaim dan is het voor het afhandelen daarvan noodzakelijk om onderzoek te doen. Uit dat onderzoek moet naar voren komen wie bij het afhandelen van de lading betrokken is geweest. Er moet kunnen worden teruggekeken in de tijd en de persoonsgegevens van die personen moeten dus zijn bewaard: minstens zolang een lading onderweg is. Het is bij een ISPS-bedrijf vooraf niet bekend hoe lang de reis van een lading gaat duren. Die duur kan bovendien ook wijzigen en het gaat daarbij om vele miljoenen ladingen/reizen per jaar. Het voorgaande betreft geen louter commercieel doel. Het is ook in het belang van de bedrijfscontinuïteit hetgeen in het belang is van de veiligheid zoals uitgelegd is in paragraaf 6.8.

In het geval een betrokkene een veiligheidsinstructie met succes heeft gevolgd, wordt dit feit opgeslagen in het toegangsmanagementsysteem. De veiligheidsinstructie dient elk jaar te worden herhaald. Is dit niet gebeurd dan wordt de toegang geweigerd. De eis om tijdig en met succes een veiligheidsinstructie te hebben gevolgd, geldt op het moment van schrijven voor alle betrokkenen, behalve voor binnenvaartbemanning, scheepsvaartbemanning en kinderen.

De bewaartermijn van een jaar geldt niet voor biometrische persoonsgegevens nu deze altijd direct worden omgezet in een versleutelde binaire code (zie paragraaf 6.13). De bewaartermijn voor biometrische gegevens bedraagt dus ‘een fractie van een seconde’. Dit met dien verstande dat de versleutelde binaire code op het pasje bewaard blijft tot het pasje door de betrokkene

wordt ingeleverd in welk geval alle gegevens op de pas binnen 24 uur na inlevering worden gewist.

6.18 Hoe worden de betrokkenen geïnformeerd?

Betrokkenen worden voortdurend over de verwerkingen in het kader van het toegangsbeleid geïnformeerd. Dit gebeurt door privacyverklaringen in de beveiligingsloge, op de balie, met waarschuwingsborden, in de veiligheidsinstructiefilm en op de website van het ISPS-bedrijf.

De informatie wordt verschaft in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. In de privacyverklaringen wordt ten minste opgenomen:

- Identiteit en contactinformatie van het ISPS-bedrijf.
- Contactinformatie van de FG of privacy officer.
- De doelen en de grondslagen van de verwerkingen.
- De gerechtvaardigde belangen van de verwerkingen.
- Om welke persoonsgegevens het gaat.
- De bron van de persoonsgegevens indien en voor zover deze niet door de betrokkene zelf zijn verstrekt.
- Eventuele (categorieën van) ontvangers van verwerkte persoonsgegevens.
- Of persoonsgegevens worden doorgegeven aan een derde land of internationale organisatie en als dat zo is welke waarborgen daarbij zijn gesteld.
- De bewaartermijn.
- De privacyrechten van een betrokkene (inzage, rectificatie, wissing, beperking, bezwaar en overdraagbaarheid, klagen).
- Dat de verstrekking van persoonsgegevens niet verplicht is, maar dat bij niet-verstrekking de toegang wordt geweigerd.
- Dat het gevolg van niet verstrekking het weigeren van toegang zal zijn.

6.19 Hoe worden de rechten van betrokkenen gewaarborgd?

Het ISPS-bedrijf heeft de verantwoordelijkheid om betrokkenen in staat te stellen hun rechten uit te oefenen.

Het ISPS-bedrijf belast ten minste één medewerker met die verantwoordelijkheid (zie ook paragraaf 6.4). Zij hanteert protocollen waarvoor standaardmodellen zijn opgenomen in bijlage 16 en stelt één emailadres open alwaar betrokkenen met hun verzoek terecht kunnen. Voorts dient de ontvangst van elk verzoek te worden bevestigd en dient iedere verzoeker zich eerst te legitimeren alvorens op het verzoek wordt beslist.

7 Bezoekers

Betrokkene
Een bezoeker is een natuurlijk persoon die niet valt onder één van de andere categorieën van betrokkenen.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding en afmelding.
- Bij aankomst op en vertrek van het terrein.

Situatie bij aanmelding en afmelding
De komst van een bezoeker wordt aangemeld door de afdeling van het ISPS-bedrijf die de bezoeker wenst te ontvangen. Deze afdeling geeft de van de bezoeker ontvangen persoonsgegevens door aan de havenbeveiliger. Dit gebeurt per mail of via een digitaal logistiek informatieplatform dat wordt beheerd door een extern bedrijf. De havenbeveiliger neemt de gegevens over uit de mail of van het informatieplatform en slaat deze op in het toegangsmanagementsysteem.

De havenbeveiliger verstrekt aan de bezoeker een toegangskaart waarmee éénmalig toegang wordt verleend tot het ISPS-bedrijf.

Bij vertrek wordt de toegangskaart ingenomen door de havenbeveiliger.

Situatie bij aankomst op en vertrek van het terrein
Een bezoeker die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen

- Persoonsgegevens worden geregistreerd in de digitale interface.
- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd, geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Adres
- Bedrijf waar degene werkzaam is
- Bedrijfsnummer
- Bedrijfsvestigingsplaats
- Camerabeelden
- Chipnummer
- Datum geldigheid VCA diploma (indien van toepassing)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Geboortedatum
- ID nummer
- ID type document
- ID geldigheid document
- Kenteken
- Naam
- Pasfoto
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type

8 Binnenvaartbemanning

Betrokkene
Een binnenvaartbemanningslid is een natuurlijk persoon die woont op en/of nautische of operationele werkzaamheden verricht op een binnenvaartschip dat lading vervoert naar of van het terrein van een ISPS-bedrijf. Een binnenvaartbemanningslid wordt in de regel opvarende genoemd. Om verwarring te voorkomen met de zeevaartbemanning, die ook opvarenden worden genoemd, wordt in deze gedragscode de term (binnenvaart)bemanningslid gehanteerd.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aankomst en vertrek van een binnenvaartschip.
- Bij van boord gaan van een binnenvaartschip om het terrein te verlaten.
- Bij aankomst op het terrein en bij het aan boord gaan van een binnenvaartschip.

Situatie bij van aankomst en vertrek van een binnenvaartschip
Bij de aankomst van een binnenvaartschip op het terrein wordt de komst gemeld aan de havenbeveiliger maar worden er geen persoonsgegevens verwerkt. Slechts de naam van binnenvaartschip wordt doorgegeven.

Bij het vertrek van een binnenvaartschip van het terrein wordt dit gemeld aan de havenbeveiliger. Er worden dan geen persoonsgegevens verwerkt.

Situatie bij van boord gaan van een binnenvaartschip om het terrein te verlaten
Wanneer een binnenvaartbemanningslid het binnenvaartschip wil verlaten dan meldt hij dit bij de havenbeveiliger. Nadat het binnenvaartbemanningslid het binnenvaartschip heeft verlaten en zich op het terrein van het ISPS-bedrijf bevindt, begeeft hij zich direct naar de uitgang van het terrein. Daar meldt hij/zij zich bij beveiligingsmedewerkers in de loge van de terminal. Daar wordt geregistreerd dat het binnenvaartbemanningslid het ISPS-bedrijf verlaat en of het binnenvaartbemanningslid voornemens is om weer terug te keren.

Situatie bij aankomst op het terrein en bij het aan boord gaan van een binnenvaartschip
In het geval dat het binnenvaartbemanningslid terugkeert en toegang wil tot het ISPS-bedrijf om weer aan boord van het binnenvaartschip te kunnen gaan, meldt hij dat bij de beveiligingsmedewerkers in de loge bij de toegangspoort van het ISPS-bedrijf. Hier wordt de identiteit gecontroleerd en wordt er gevraagd naar de reden van zijn wens om toegang te krijgen. Het binnenvaartbemanningslid zelf of de beveiligingsmedewerker in de loge informeert het binnenvaartschip waarna het binnenvaartbemanningslid toegang wordt verleend tot het terrein om aan boord van het binnenvaartschip te kunnen gaan.

Verwerkingen

- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd,
- geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Visuele controle ID bewijs.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Camerabeelden
- Geboortedatum
- ID nummer
- ID type document
- ID geldigheid document
- Kenteken
- Naam
- Naam binnenvaartschip
- Telefoonnummer
- Zakelijk adres

PORT PRIVACY

9 Bootmannen en sjorders

Betrokkene
Een bootman is een natuurlijk persoon die aangesloten is bij een bootliedenorganisatie. Een bootman (of 'roeier') is belast met het vast- en losmaken van een schip. Een sjorder is een natuurlijk persoon die werkzaam is bij een sjorderbedrijf. Een sjorder is belast met het zeevast zetten en losmaken van containers aan boord van een schip.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding en afmelding.
- Bij aankomst op en vertrek van een terrein.

Situatie bij aanmelding en afmelding

De komst van een bootman/sjorder wordt aangemeld door de afdeling van het ISPS-bedrijf die belast is met de logistieke inhuur en planning van de schepen. Deze afdeling geeft de van de bootman/sjorder ontvangen persoonsgegevens door aan de havenbeveiliger. Dit gebeurt per mail of via een digitaal logistiek informatieplatform dat wordt beheerd door een extern bedrijf. De havenbeveiliger neemt de gegevens over uit de mail of van het informatieplatform en slaat deze op in het toegangsmanagementsysteem.

De havenbeveiliger verstrekt aan de bootman/sjorder een toegangskaart waarmee gedurende een bepaalde periode toegang wordt verleend tot het ISPS-bedrijf.

Bij vertrek wordt de toegangskaart ingenomen door de havenbeveiliger.

Situatie bij aankomst op en vertrek van het terrein

Een bootman/sjorder die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Biometrische verificatie
In het geval een bootman/sjorder zich middels biometrische verificatie toegang wil tot het terrein of het terrein wil verlaten, geldt dat hij behalve zijn toegangskaart ook zijn (aderpatroon van) zijn vinger of hand aan een daarvoor geschikt uitleesapparaat aanbiedt. Ook dit apparaat is verbonden met het toegangsmanagementsysteem. Het systeem maakt met het aderpatroon een berekening en die wordt vergeleken met de berekening die door de leverancier van het

managementsysteem op de toegangskaart is gezet. Vervolgens vergelijkt het systeem deze gegevens met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen
- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd, geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens
- Bedrijf waar degene werkzaam is
- Bedrijfsnummer
- Bedrijfsvestigingsplaats
- Biometrische gegevens met het oog op unieke identificatie
- Camerabeelden
- Chipnummer
- Datum geldigheid VCA diploma (indien van toepassing)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Geboortedatum
- Kenteken
- Naam
- Pasfoto
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type
- Zakelijk adres

10 Externe arbeidskrachten

Betrokkene
Een externe arbeidskracht is een natuurlijk persoon die voor het ISPS-bedrijf werkzaam is op basis van 'inhuur': inlening, aanneming van werk of een overeenkomst van opdracht (uitzendkrachten, gedetacheerden, aannemers, ZZP-ers, etc.).

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding.
- Bij aankomst op en vertrek van het terrein.
- Bij afmelding.

Situatie bij aanmelding
De komst van een externe arbeidskracht wordt aangemeld door de afdeling van het ISPS-bedrijf die de externe arbeidskracht heeft ingehuurd. Deze afdeling geeft de van de externe arbeidskracht of van diens werkgever/opdrachtgever ontvangen persoonsgegevens door aan de havenbeveiliger. Dit gebeurt per mail of via een digitaal logistiek informatieplatform dat wordt beheerd door een extern bedrijf. De havenbeveiliger neemt de gegevens over uit de mail of van het informatieplatform en slaat deze op in het toegangsmanagementsysteem. Aan de externe arbeidskracht wordt een toegangsprofiel toegekend.

De havenbeveiliger verstrekt aan de externe arbeidskracht een toegangskaart waarmee gedurende de inhuurperiode toegang wordt verleend tot het ISPS-bedrijf.

Situatie bij aankomst op en vertrek van het terrein
Een externe arbeidskracht die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

PORT PRIVACY

Situatie bij afmelding van een externe arbeidskracht

De betreffende afdeling van het ISPS bedrijf meldt bij de havenbeveiliger dat de inhuur stopt en per wanneer dat het geval is. De havenbeveiliger noteert dit in het toegangsmanagementsysteem zodat de toegangskaart vanaf die dag geen toegang meer zal geven. De externe arbeidskracht wordt gevraagd de pas in te leveren waarna de persoonsgegevens van de pas worden verwijderd.

Verwerkingen

- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd,
- geregistreerd in en verwijderd uit in het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Afdeling waar degene werkzaam is
- Camerabeelden
- Chipnummer
- Datum geldigheid VCA diploma (indien van toepassing, namelijk wanneer een VCA diploma vereist voor zijn functie)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Geboortedatum
- Kenteken
- Naam
- Pasfoto
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type
- Zakelijk adres

11 Kinderen

Betrokkene
Een kind is een natuurlijke persoon die de leeftijd van 18 jaar nog niet heeft bereikt.

Situatie
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aankomst op en vertrek van het terrein.

Situatie bij aankomst op en vertrek van het terrein.
De komst van een kind van een binnenvaartbemanningslid wordt bij de havenbeveiliger aangemeld door het binnenvaartbemanningslid die zijn kind van of aan boord wil brengen. Dit gebeurt per mail of per telefoon. De havenbeveiliger neemt de gegevens over uit het telefoongesprek of de mail en slaat deze op in het toegangsmanagementsysteem.

Kinderen die niet door een binnenvaartbemanningslid worden aangemeld bij de havenbeveiliger worden geweigerd, tenzij er een uitzondering voor wordt gemaakt zoals in het geval van een schoolexcursie in welk geval zij worden beschouwd als ‘bezoeker’ (zie hoofdstuk 7) maar slechts de onderstaande persoonsgegevens worden verwerkt.

Verwerkingen

- Persoonsgegevens worden ontvangen, opgenomen, gecontroleerd en geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Naam
- Camerabeelden

PORT PRIVACY

12 Leveranciers en shipchandlers

Betrokkene
Een leverancier is een natuurlijk persoon die werkzaam is voor een leveranciersbedrijf dat producten of diensten levert aan een ISPS-bedrijf (waarbij het niet de kernactiviteiten betreft die door werknemers en externe arbeidskrachten worden verricht). Een shipchandler is een natuurlijk persoon die werkzaam is voor een scheepsleveranciersbedrijf dat in opdracht van een rederij, een scheepsagent of het schip zelf, producten of diensten levert aan een schip dat ligt aangemeerd bij een terminal.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding en afmelding.
- Bij aankomst op en vertrek van het terrein.

Situatie bij aanmelding en afmelding

De komst van een leverancier wordt aangemeld door de afdeling van het ISPS-bedrijf die de leverancier/shipchandler wenst te ontvangen. De komst van een shipchandler wordt aangemeld door het schip (SSO), een scheepsagent (CSO) of de rederij van het schip die de shipchandler wenst te ontvangen. De van de leverancier/shipchandler ontvangen persoonsgegevens worden doorgegeven aan de havenbeveiliger. Dit gebeurt per mail of via een digitaal logistiek informatieplatform dat wordt beheerd door een extern bedrijf. De havenbeveiliger neemt de gegevens over uit de mail of van het informatieplatform en slaat deze op in het toegangsmanagementsysteem. Aan de leverancier/shipchandler wordt een toegangsprofiel toegekend.

De havenbeveiliger verstrekt aan de leverancier/shipchandler een toegangskaart waarmee éénmalig of gedurende een bepaalde periode toegang wordt verleend tot het ISPS-bedrijf.

Bij vertrek wordt de toegangskaart ingenomen door de havenbeveiliger.

Situatie bij aankomst op en vertrek van het terrein

Een leverancier/shipchandler die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen
- Persoonsgegevens worden geregistreerd in de digitale interface.
- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd,
- geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens
- Bedrijf waar degene werkzaam is
- Bedrijfsnummer
- Bedrijfsvestigingsplaats
- Datum geldigheid VCA diploma (indien van toepassing)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Camerabeelden
- Chipnummer
- Geboortedatum
- ID nummer
- ID type document
- ID geldigheid document
- Kenteken
- Naam
- Pasfoto
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type
- Zakelijk adres

PORT PRIVACY

13 Onbevoegd aanwezigen

Betrokkene
Een onbevoegd aanwezige is een natuurlijk persoon zonder bevoegdheid om op het terrein aanwezig te zijn, dat wil zeggen zonder voorafgaande aanmelding bij en/of zonder goedkeuring van het ISPS-bedrijf.

Situatie
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij vertrek van het terrein.

Situatie bij vertrek van het terrein

Wanneer een natuurlijk persoon onbevoegd aanwezig blijkt te zijn, wordt diens identiteit gecontroleerd en worden zijn persoonsgegevens geregistreerd in het toegangsmanagementsysteem en wordt melding gemaakt bij het ISPS-meldpunt van de politie. Vervolgens wordt de betrokkene het terrein afgeleid.

Verwerkingen

- Persoonsgegevens worden visueel gecontroleerd aan de hand van het ID bewijs.
- Persoonsgegevens worden geregistreerd in het toegangsmanagementsysteem.
- Persoonsgegevens worden gemeld aan het ISPS-meldpunt van de politie.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Camerabeelden
- Geboortedatum
- Kenteken
- Naam

14 Overheidspersoneel

Betrokkene
Overheidspersoneel betreft natuurlijk personen in dienst van een (semi-)overheidsdienst, ook wel ambtenaren genoemd. De ambtenaren die in deze code worden genoemd, treden op als:

- Toezichthouders zoals bedoeld in de Algemene Wet Bestuursrecht.
- Opsporingsambtenaren zoals bedoeld in het Wetboek van Strafvordering.
- Ambtenaren zoals bedoeld in de Wet op de Inlichtingen- en Veiligheidsdiensten 2002.
- Ambtenaren zoals bedoeld in de Algemene Douanewet.

De genoemde ambtenaren mogen niet beperkt worden door de beveiligingsplannen van havenfaciliteiten of schepen. Dit betekent dat zij niet verplicht kunnen worden om medewerking te verlenen aan vormen van toegangscontrole. Waar mogelijk en wenselijk volgen de genoemde ambtenaren echter de uitgangspunten van het Protocol Toegang Havenfaciliteiten voor Overheidsambtenaren (bijlage 12).

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aankomst op en vertrek van het terrein.

Situatie bij aankomst op en vertrek van het terrein
Een ambtenaar die toegang wil tot het terrein of het terrein wil verlaten, volgt het Protocol Toegang Havenfaciliteiten voor Overheidsambtenaren dat in onderdeel B een instructie geeft hoe overheidsambtenaren moeten handelen bij een toegangscontrole (bijlage 12).

In voorkomende gevallen wordt gebruik gemaakt van een biometrische toegangskaart. In dat geval heeft de betreffende overheidsdienst daartoe een overeenkomst gesloten met de leverancier/beheerder van het systeem t.b.v. biometrische verificatie. Het ISPS-bedrijf is hierbij, anders dan bij de andere categorieën van betrokkenen, geen partij en dus ook niet verwerkingsverantwoordelijk.

Biometrische verificatie
In het geval een ambtenaar zich middels biometrische verificatie toegang wil verschaffen tot het terrein of het terrein wil verlaten, geldt dat hij behalve zijn toegangskaart ook zijn (aderpatroon van) zijn vinger of hand aan een daarvoor geschikt uitleesapparaat aanbiedt. Ook dit apparaat is verbonden met het toegangsmanagementsysteem. Het systeem maakt met het aderpatroon een berekening en die wordt vergeleken met de berekening die door de leverancier van het managementsysteem op de toegangskaart is gezet. Vervolgens vergelijkt het systeem deze gegevens met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen
Het bekendmaken van zichzelf en de dienst waarvoor zij werkzaam zijn en het tonen van het legitimatiebewijs (zonder dat daar een kopie van mag worden gemaakt), betreffen geen verwerkingen van persoonsgegevens.

Ook wanneer een biometrische pas en een vinger of de hand van de ambtenaar wordt aangeboden, vindt er geen verwerking plaats door of namens het ISPS-bedrijf (maar door de leverancier/beheerder van het systeem t.b.v. biometrische verificatie).

Wanneer een ambtenaar de bezoekersregistratie tekent, wordt hij gezien als een ‘bezoeker’ en vindt er wel een verwerking van persoonsgegevens plaats (zie hoofdstuk 7).

Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens
- Biometrische gegevens met het oog op unieke identificatie
- Camerabeelden
- Kenteken
- Naam

15 Scheepsbemanning

Betrokkene
Een scheepsbemanningslid is een natuurlijk persoon die werkzaam is op een schip dat een ISPS-bedrijf aandoet of wil aandoen. Een scheepsbemanningslid wordt in de regel opvarende genoemd. Om verwarring te voorkomen met de binnenvaartbemanning die ook opvarenden worden genoemd, wordt in deze gedragscode de term scheepsbemanningslid gehanteerd.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding van een schip.
- Bij van boord gaan om het terrein te verlaten.
- Bij aankomst en bij het aan boord gaan van een schip.
- Bij afmelding en vertrek van een schip.

Situatie bij aanmelding van een schip
Wanneer een schip een terminal wil aandoen, meldt het zich aan bij de havenbeveiliger met een pre-arrival-document. Dit document bevat diverse gegevens waaronder de scheepsbemanningslijst van het te arriveren schip. De scheepsbemanningslijst bevat persoonsgegevens.

De melding kan geschieden per mail door het schip (SSO) of door de scheepsagent (CSO). De melding kan ook geschieden via een digitaal informatieplatform dat wordt beheerd door een externe partij. De terminal ontvangt de aanmelding via de mail of door dit af te lezen op de interface van bedoeld informatieplatform. Alleen de terminal waar het schip wil aanmeren, heeft toegang tot deze gegevens op het informatieplatform.

De persoonsgegevens op de scheepsbemanningslijst worden door de havenbeveiliger opgeslagen in haar toegangsmanagementsysteem. Is de aanmelding per mail geschied, dan wordt de mail geprint en opgeslagen in een fysieke map en voorts digitaal opgeslagen in het mailaccount van de terminal.

Situatie bij van boord gaan van een schip om het terrein te verlaten
Wanneer een scheepsbemanningslid het schip wil verlaten dan meldt hij dit bij de havenbeveiliger van de terminal. Nadat het scheepsbemanningslid het schip heeft verlaten en zich op het terrein van de terminal bevindt, begeeft hij zich direct naar de uitgang van het terrein. Daar meldt hij/zij zich bij beveiligingsmedewerkers in de loge van de terminal. Hier wordt geregistreerd dat het scheepsbemanningslid de terminal verlaat en/of het scheepsbemanningslid voornemens is om weer terug te keren naar de terminal.

PORT PRIVACY

Situatie bij aankomst op het terrein en bij het aan boord gaan van een schip

In het geval dat het scheepsbemanningslid terugkeert en toegang wil tot de terminal om weer aan boord van het schip te kunnen gaan, meldt hij dat bij de beveiligingsmedewerkers in de loge bij de toegangspoort van de terminal. Hier wordt zijn identiteit gecontroleerd en wordt gevraagd naar de reden van zijn wens om toegang te krijgen. Er wordt gecontroleerd of het scheepsbemanningslid op de scheepsbemanningslijst van het betreffende schip staat vermeld waarna het scheepsbemanningslid toegang wordt verleend tot het terrein om aan boord van het schip te kunnen gaan.

Situatie bij afmelding en vertrek van een schip

Wanneer het schip wil vertrekken, meldt de SSO van het schip dit bij de havenbeveiliger. Daarbij wordt de scheepsbemanningslijst gecontroleerd of alle scheepsbemanningsleden aan boord zijn. Na controle kan het schip vertrekken.

Verwerkingen

- Persoonsgegevens worden geregistreerd in de digitale interface.
- Persoonsgegevens worden opgevraagd, ontvangen per mail of opgehaald van een digitaal informatieplatform, opgenomen, gecontroleerd, geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen in een fysieke map.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Camerabeelden
- ID nummer
- ID type document
- ID geldigheid document
- Geboortedatum
- Naam
- Naam schip

16 Vrachtautochauffeurs

Betrokkene
Een vrachtautochauffeur is een natuurlijk persoon die met een vrachtauto lading vervoert naar of van het terrein van een ISPS-bedrijf.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding.
- Bij aankomst op en vertrek van het terrein.

Situatie bij aanmelding

De komst van een vrachtautochauffeur wordt aangemeld door de afdeling van het ISPS-bedrijf die belast is met de logistieke inhuur en planning van vrachtauto's. Deze afdeling geeft de van de vrachtautochauffeur of dienst werkgever/opdrachtgever ontvangen persoonsgegevens door aan de havenbeveiliger. Dit gebeurt per mail of via een digitaal logistiek informatieplatform dat wordt beheerd door een extern bedrijf. De havenbeveiliger neemt de gegevens over uit de mail of van het informatieplatform en slaat deze op in het toegangsmanagementsysteem.

De havenbeveiliger verstrekt aan de vrachtautochauffeur een toegangskaart waarmee éénmalig of gedurende een bepaalde periode toegang wordt verleend tot het ISPS-bedrijf.

Situatie bij aankomst op en bij vertrek van het terrein

Een vrachtautochauffeur die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd.

Biometrische verificatie
In het geval een vrachtautochauffeur zich middels biometrische verificatie toegang wil tot het terrein of het terrein wil verlaten, geldt dat hij behalve zijn toegangskaart ook zijn (aderpatroon van) zijn vinger of hand aan een daarvoor geschikt uitleesapparaat aanbiedt. Ook dit apparaat is verbonden met het toegangsmanagementsysteem. Het systeem maakt met het aderpatroon een berekening en die wordt vergeleken met de berekening die door de leverancier van het managementsysteem op de toegangskaart is gezet. Vervolgens vergelijkt het systeem deze gegevens met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de

gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen
- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd,
- geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens
- Bedrijf waar degene werkzaam is
- Bedrijfsnummer
- Bedrijfsvestigingsplaats
- Biometrische gegevens met het oog op unieke identificatie
- Camerabeelden
- Chipnummer
- Datum geldigheid VCA diploma (indien van toepassing)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Geboortedatum
- ID nummer
- ID type document
- ID geldigheid document
- Kenteken
- Naam
- Pasfoto
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type
- Zakelijk adres

17 Vrachttreinpersoneel

Betrokkene
Alle op de vrachttrein aanwezige natuurlijke personen die in opdracht van het ISPS-bedrijf het terrein van de terminal via het spoor betreden.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij aanmelding.
- Bij aankomst op en vertrek van het terrein.
- Bij aankomst op het terrein en bij het plaatsnemen in de vrachttrein.

Situatie bij aanmelding
De afdeling van het ISPS-bedrijf die belast is met de logistieke inhuur en planning van de vrachttreinen, ontvangt de persoonsgegevens van diegene die het ISPS-bedrijf wil bezoeken en geeft deze door aan de havenbeveiliger die de persoonsgegevens opneemt in het toegangsmanagementsysteem.

Situatie bij aankomst op en vertrek van het terrein
Wanneer de vrachttrein bij het ISPS-bedrijf aankomt en toegang wil tot het terrein, meldt het vrachttreinpersoneel zich bij de spoorpoort. Aldaar controleert het ISPS-bedrijf de naam van het bedrijf van de vrachttrein en de voorwaarden om toegang te verkrijgen. De persoonsgegevens van het vrachttreinpersoneel en de reden van het bezoek worden opgeslagen in het toegangsmanagementsysteem. De spoorpoort wordt door tussenkomst van het havenbeveiligingsbedrijf handmatig geopend wanneer een vrachttrein bij de spoorpoort aankomt. De aanwezigheid wordt geregistreerd.

Bij het vertrek vanaf het terrein handelt het vrachttreinpersoneel op dezelfde wijze als bij aankomst. Ook dan controleert de havenbeveiliger in het systeem de gegevens en wordt het vertrek geregistreerd.

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

PORT PRIVACY

Situatie bij aankomst op het terrein en bij het plaatsnemen in de vrachttrein

In het geval het vrachttreinpersoneel toegang wil tot het ISPS-bedrijf om plaats te nemen in de vrachttrein, meldt hij/zij dat bij de beveiligingsmedewerkers in de loge bij de toegangspoort van het ISPS-bedrijf. Hier wordt zijn identiteit gecontroleerd en wordt er gevraagd naar de reden van zijn wens om toegang te krijgen.

Verwerkingen

- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen, gecontroleerd,
- geregistreerd in en verwijderd uit het toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens

- Bedrijf waar degene werkzaam is
- Bedrijfsnummer
- Bedrijfsvestigingsplaats
- Camerabeelden
- Datum geldigheid VCA diploma (indien van toepassing)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Geboortedatum
- Naam
- Telefoonnummer
- Zakelijk adres

18 Werknemers

Betrokkene
Een werknemer is een natuurlijk persoon die een arbeidsovereenkomst heeft met het ISPS-bedrijf.

Situaties
In het kader van de toegangscontrole en de daar aan gerelateerde beveiligingsdoeleinden zijn er, naast het feit dat van de betrokkene camerabeelden worden gemaakt, verschillende situaties te onderscheiden waarin een ISPS-bedrijf persoonsgegevens van deze categorie van betrokkenen verwerkt of laat verwerken:

- Bij in- en uitdiensttreding.
- Bij aankomst op en vertrek van het terrein.

Situatie bij in- en uitdiensttreding

Wanneer een werknemer in dienst treedt van een ISPS-bedrijf ontvangt de HR-afdeling van het ISPS-bedrijf persoonsgegevens van de nieuwe werknemer en geeft deze door aan de havenbeveiliger. De havenbeveiliger zet de gegevens van de werknemer in het toegangsmanagementsysteem. Aan de werknemer wordt een toegangsprofiel toegekend. Er wordt een toegangskaart aangemaakt. De toegangskaart wordt vervolgens aan de werknemer verstrekt.

Bij uitdiensttreding worden de persoonsgegevens van de toegangskaart verwijderd waardoor deze onbruikbaar wordt.

Situatie bij aankomst op en vertrek van het terrein

Een werknemer die toegang wil tot het terrein of het terrein wil verlaten, houdt zijn toegangskaart tegen een bij de toegangspoort geplaatst uitleesapparaat. Dit apparaat is verbonden met het toegangsmanagementsysteem.

Bij het uitlezen van de toegangskaart vergelijkt het systeem de persoonsgegevens op de toegangskaart met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt de weigering geregistreerd.

Biometrische verificatie
In het geval een werknemer zich middels biometrische verificatie toegang wil tot het terrein of het terrein wil verlaten, geldt dat hij behalve zijn toegangskaart ook zijn (aderpatroon van) zijn vinger of hand aan een daarvoor geschikt uitleesapparaat aanbiedt. Ook dit apparaat is verbonden met het toegangsmanagementsysteem. Het systeem maakt met het aderpatroon een berekening en die wordt vergeleken met de berekening die door de leverancier van het managementsysteem op de toegangskaart is gezet. Vervolgens vergelijkt het systeem deze gegevens met de persoonsgegevens die in het systeem zijn opgeslagen. Wanneer de

gegevens overeenkomen, wordt de aankomst of het vertrek geregistreerd. Komen de gegevens niet overeen dan wordt geen toegang verleend en wordt de weigering geregistreerd

Veiligheidsinstructie
Bij een eerste bezoek kan de betrokkene worden verplicht om een veiligheidsinstructie te volgen en te slagen voor de bijbehorende toets. In het toegangsmanagementsysteem wordt dan de datum geregistreerd waarop de veiligheidsinstructie is gevolgd en of de bijbehorende toets is behaald. Ieder jaar moet deze veiligheidsinstructie opnieuw worden gevolgd.

Verwerkingen
- Persoonsgegevens worden opgevraagd, ontvangen, opgenomen,
- gecontroleerd, geregistreerd in en verwijderd uit het
- toegangsmanagementsysteem.
- Persoonsgegevens worden opgeslagen op een toegangskaart.
- Persoonsgegevens worden van de toegangskaart verwijderd.
- Persoonsgegevens worden geregistreerd door het camerasysteem.

Persoonsgegevens
- Afdeling waar degene werkzaam is
- Biometrische gegevens met het oog op de unieke identificatie van een persoon
- Camerabeelden
- Chipnummer
- Datum geldigheid VCA diploma (indien van toepassing, namelijk wanneer een VCA diploma vereist voor zijn functie)
- Datum waarop de veiligheidsinstructie/toets is afgenomen
- Functie
- Geboortedatum
- ID nummer
- ID type document
- ID geldigheid document
- Kenteken
- Pasfoto
- Privé adres
- Privé mailadres
- Telefoonnummer
- Toegangskaart nummer
- Toegangskaart geldigheid
- Toegangskaart type

PORT PRIVACY

19 Gedragsregels

Verwerkingsverantwoordelijk (paragraaf 6.1)
Het ISPS-bedrijf is en handelt als verwerkingsverantwoordelijke ten aanzien van de verwerking van persoonsgegevens in het kader van haar toegangsbeleid.

Verwerkersovereenkomsten en overeenkomsten wegens gezamenlijke verantwoordelijkheid (paragraaf 6.2 en 6.3)
Het ISPS-bedrijf sluit een verwerkersovereenkomst met het havenbeveiligingsbedrijf dat ten behoeve van haar toegangsbeleid persoonsgegevens verwerkt.

Het ISPS-bedrijf sluit een verwerkersovereenkomst met de leverancier van het toegangsmanagementsysteem die ten behoeve van haar toegangsbeleid persoonsgegevens verwerkt.

Het ISPS-bedrijf sluit voorts een overeenkomst met de leverancier van het toegangsmanagementsysteem om daarmee de afspraken te bevestigen die zijn gemaakt vanwege de gezamenlijke verantwoordelijkheid voor de verwerking van persoonsgegevens in het kader van het toegangsbeleid.

Het ISPS-bedrijf sluit een verwerkersovereenkomst met de leverancier van het camerasysteem die ten behoeve van haar toegangsbeleid persoonsgegevens verwerkt.

Het ISPS-bedrijf sluit een verwerkersovereenkomst met de leverancier van het digitale informatieplatform die ten behoeve van haar toegangsbeleid persoonsgegevens verwerkt.

Het ISPS-bedrijf gaat, steeds wanneer er in het kader van haar toegangsbeleid een ander bedrijf wordt ingeschakeld, na of daarmee een verwerkersovereenkomst en/of een overeenkomst wegens gezamenlijke verwerkingsverantwoordelijkheid moet worden gesloten.

Privacy Officer (paragraaf 6.4)
Het ISPS-bedrijf belast één medewerker met de verantwoordelijkheid om de Gedragscode na te leven.

Functionaris Gegevensbescherming (paragraaf 6.5)
Het ISPS-bedrijf besluit of er een FG wordt aangesteld en motiveert dit in haar privacybeleid.

Verwerkingsregister (paragraaf 6.6)
Het ISPS-bedrijf voert een verwerkingsregister ten aanzien van haar toegangsbeleid. Zij draagt er voortdurend zorg voor dat dit register actueel is.

Privacybeleid (paragraaf 6.7)

Het ISPS-bedrijf legt haar privacybeleid in het kader van haar toegangsbeleid schriftelijk vast. Zij draagt er voortdurend zorg voor dat dit beleid doeltreffend is. In het beleid wordt gemotiveerd wat de doelen en de grondslagen van het toegangsbeleid zijn.

Meerdere betrokkenen (paragraaf 6.9)
Het ISPS-bedrijf onderscheidt in de uitvoering van haar toegangsbeleid meerdere situaties en verschillende categorieën van betrokkenen.

Verschillende verwerkingen in verschillende situaties (paragraaf 6.10, 6.11 en 6.12 en hoofdstukken 7 t/m 18)
Het ISPS-bedrijf stelt in elke situatie vast om welke categorie van betrokkenen het gaat en welke in de Gedragscode beschreven situatie aan de orde is. Zodra dit is vastgesteld, verwerkt het ISPS-bedrijf de persoonsgegevens op de wijze zoals is beschreven in het betreffende hoofdstuk (hoofdstukken 7 t/m 18).

Kinderen (hoofdstuk 11)
Het ISPS-bedrijf weigert de toegang van kinderen tot haar terrein, behalve de kinderen van binnenvaartbemanning indien daar om wordt verzocht.

Biometrische verificatie (paragraaf 6.13 en 6.15)
Het ISPS-bedrijf dat gebruik maakt van biometrische verificatie doet louter zaken met een leverancier van het toegangsmanagementsysteem die een DPIA heeft uitgevoerd op haar dienstverlening en voert voorts ook zelf een DPIA uit.

DPIA (paragraaf 6.14)
Het ISPS-bedrijf voert een DPIA uit indien en zodra er, gezien alle omstandigheden, sprake is van (nieuwe) verwerkingen met een hoog risico voor de rechten en vrijheden van betrokkenen; bijvoorbeeld wanneer databestanden worden gekoppeld of gecombineerd, er nieuwe technologie wordt toegepast of er sprake is van doorgifte naar landen buiten de Europese Unie.

Het ISPS-bedrijf voert in ieder geval een DPIA uit ten aanzien van haar camerabeleid.

Het ISPS-bedrijf actualiseert de uitgevoerde DPIA's zodra de omstandigheden wijzigen en daar aanleiding toe is, en minstens één keer per jaar.

Beveiliging (paragraaf 6.16)
Het ISPS-bedrijf neemt passende beveiligingsmaatregelen en maakt in ieder geval gebruik van:

- Data encryptie
- Data back up
- Opslag van data bij een secured data center
- Offsite data back up
- Network port security
- Network authentication
- Network segmentation
- Antivirus en antimalware

- Firewalling
- Role based access control
- Logging

Voorts geldt in ieder geval het volgende:

- Het ISPS-bedrijf voldoet aan de eisen van de ISO-norm 27001 voor informatiebeveiliging en de ISO-norm 27701 voor privacy.
- Het ISPS-bedrijf maakt alleen gebruik van leveranciers van toegangsmanagementsystemen die voldoen aan de eisen van de ISO-norm 27001 voor informatiebeveiliging.
- Alle digitale bestanden en systemen waarin persoonsgegevens zijn opgeslagen, worden beveiligd met een wachtwoord. Er wordt multifactorauthenticatie toegepast.
- Wachtwoorden zijn alleen bekend bij de personen die de gegevens nodig hebben om hun functie en de daar bijbehorende taken goed uit te kunnen voeren.
- Wachtwoorden worden periodiek gewijzigd.
- Digitale systemen worden periodiek gecontroleerd op virussen en andere onregelmatigheden.
- Digitale systemen worden voortdurend geüpdatet met de nieuwste versie van de betreffende software.
- Digitale systemen draaien op servers die in de Europese Economische Ruimte (EER) staan zodat persoonsgegevens niet daarbuiten worden opgeslagen.
- Havenbeveiligers worden elke 3 jaar gescreend door het Ministerie van Justitie (Justis).
- ISPS-bedrijven hanteren een protocol aan de hand waarvan wordt bepaald of en wanneer het datalek wordt gemeld aan de AP en/of aan betrokkenen (zie bijlage 16).
- Wordt gebruik gemaakt van biometrische verificatie dan wordt het biometrische template enkel opgeslagen op de toegangskaart en niet in de centrale systemen.

Datalek (paragraaf 6.16)
Het ISPS-bedrijf hanteert een protocol voor het geval er sprake is van een datalek aan de hand waarvan een datalek wel of niet wordt gemeld bij de AP en/of betrokkenen.

Het ISPS-bedrijf voert het beleid dat men intern (potentiële) datalekken meldt aan de medewerker die is belast met de verantwoordelijkheid voor de naleving van de Gedragscode.

Bewaartermijn (paragraaf 6.17)
Het ISPS-bedrijf hanteert voor alle persoonsgegevens die in het kader van haar toegangsbeleid een bewaartermijn van één jaar. Na afloop van de bewaartermijn worden alle persoonsgegevens gewist uit alle systemen die in het kader van haar toegangsbeleid worden gebruikt.

Dit geldt alleen niet voor de persoonsgegevens van kinderen. De persoonsgegevens van kinderen worden direct uit het toegangsmanagementsysteem verwijderd zodra het kind aan of van boord is van het binnenvaartschip.

De bewaartermijn van een jaar geldt voorts niet voor biometrische persoonsgegevens nu deze altijd direct worden omgezet in een versleutelde binaire code, met dien verstande dat de

versleutelde binaire code op het pasje bewaard blijft tot het pasje door de betrokkene wordt ingeleverd in welk geval alle gegevens op de pas binnen 24 uur na inlevering worden gewist.

Informatie (paragraaf 6.18)
Het ISPS-bedrijf informeert alle betrokkenen over de verwerking van persoonsgegevens in het kader van haar toegangsbeleid door privacyverklaringen in de beveiligingsloge, op de balie, met waarschuwingsborden, in de veiligheidsinstructiefilm en op de website.

Privacyrechten (paragraaf 6.19)
Het ISPS-bedrijf hanteert protocollen voor het geval een betrokkene gebruik maakt van zijn of haar privacyrechten.

Toezicht en audits (hoofdstuk 20)
Het ISPS-bedrijf aanvaardt het externe onafhankelijke toezichthoudend orgaan zoals opgenomen in hoofdstuk 20.

Het ISPS-bedrijf laat minstens één maal per jaar een audit uitvoeren op de naleving van de gedragscode conform hetgeen daarvoor is bepaald in hoofdstuk 20 en bijbehorende bijlagen.

20 Beheer, toezicht en deelnemen

In dit hoofdstuk is opgenomen hoe het beheer van de Gedragscode en het toezicht op naleving daarvan is geregeld. Hier zijn drie organisaties bij betrokken: de beheerder van de Gedragscode, het raadgevend orgaan en het toezichthoudend orgaan. Uit dit hoofdstuk volgt welke taken en verantwoordelijkheden zij hebben en hoe de organisaties zich tot elkaar verhouden.

Ook is in dit hoofdstuk opgenomen welke procedure een ISPS-bedrijf moet volgen om te kunnen deelnemen aan de Gedragscode. Tot slot zijn de nodige contactgegevens aan dit hoofdstuk toegevoegd.

20.1 Beheerder van de gedragscode (Port Privacy)

De beheerder van de gedragscode is haar intellectueel eigenaar: Port Privacy. De beheerder heeft de navolgende taken.

Goed functionerende Gedragscode
Het is de taak van de beheerder om de Gedragscode goed te laten functioneren en dus ook om deze actueel te houden. Periodiek verricht zij daartoe onderzoek naar alle relevante ontwikkelingen en gebeurtenissen, zoals wetswijzigingen, Guidelines van de EDPB, beleidslijnen van de AP, jurisprudentie, adviezen van het CCvD, vragen van het toezichthoudend orgaan, tips, wensen, incidenten en/of klachten. De bevindingen worden periodiek en minstens éénmaal per jaar besproken met het raadgevend orgaan en het toezichthoudend orgaan.

Om de Gedragscode goed te laten functioneren, kan de beheerder besluiten tot wijziging van de Gedragscode. Over het voornemen tot wijziging wordt overleg gevoerd met het raadgevend orgaan en een wijziging wordt pas doorgevoerd na goedkeuring door de AP. Wijzigingen van de Gedragscode zijn bindend voor de aangesloten bedrijven.

Beoordelingscriteria
Het is de taak van de beheerder om de beoordelingscriteria vast te stellen die door het toezichthoudend orgaan worden gebruikt bij het uitvoeren van audits om te bepalen of een ISPS-bedrijf mag (blijven) deelnemen aan de Gedragscode.

Deelnemersregister
Het is de taak van de beheerder om een register te voeren met alle deelnemers aan de Gedragscode. Per deelnemend ISPS-bedrijf wordt in ieder geval geregistreerd: de naam van het bedrijf, de naam van de contactpersoon, de contactgegevens en de aanvangsdatum van deelname. Port Privacy zal ten behoeve van het register een openbaar toegankelijke website inrichten.

Benoeming CCvD
Het is de taak van de beheerder om de leden van het CCvD te benoemen en te registreren wie lid zijn van het CCvD en welke organisaties zij vertegenwoordigen. Zie paragraaf ‘raadgevend orgaan’.

Eindtermen voor accreditatie toezichthoudend orgaan
Het is de taak van de beheerder om de eindtermen te bepalen voor de accreditatie van een toezichthoudend orgaan zodat vooraf helder is of een organisatie als toezichthoudend orgaan kan fungeren.

Contact onderhouden met raadgevend orgaan en toezichthoudend orgaan
Het is de taak van de beheerder om periodiek contact te onderhouden met het raadgevend orgaan en met het toezichthoudend orgaan. Dit gebeurt ten minste éénmaal per jaar in een door de beheer te faciliteren vergadering waarbij zowel de beheerder, als het raadgevend en toezichthoudend orgaan bijeenkomen.

Contact onderhouden met de AP
Het is de taak van de beheerder om periodiek contact te onderhouden met de AP. Dit gebeurt in ieder geval ten aanzien van de goedkeuring van de Gedragscode en ten behoeve van de registratie door de AP van de deelnemende bedrijven.

Informatievoorziening
Het is de taak van de beheerder om de verschillende categorieën van belanghebbenden, waaronder de ISPS-bedrijven en de betrokkenen, over de Gedragscode te informeren.

Klachten
Het is de taak van de beheerder om eventuele klachten te laten behandelen door de aangewezen organisatie en aldus om eventuele klagers daar naar door te verwijzen. Betreft het een klacht over de inhoud of het functioneren van de Gedragscode dan neemt de beheerder deze zelf in behandeling. Daartoe stelt de beheerder een klachtenregeling op.

20.2 Raadgevend orgaan (Centraal College van Deskundigen)

De beheerder van de Gedragscode heeft als raadgevend orgaan het Centraal College van Deskundigen (CCvD) ingesteld.

Samenstelling
Het CCvD wordt samengesteld uit vertegenwoordigers van de bij de Gedragscode belanghebbende partijen; de leden van de huidige werkgroep worden hiervoor benaderd (zie hoofdstuk 5). Het doel hiervan is dat alle categorieën van belanghebbenden inspraak hebben in het functioneren van de Gedragscode.

Benoeming en zittingsduur
De beheerder benoemt de leden van het CCvD en registreert wie lid is en welke organisaties zij vertegenwoordigen. Bij de benoeming van een lid van het CCvD stelt de beheerder vast of deze voldoende deskundig is met betrekking tot de in het CCvD te behandelen onderwerpen. Tevens draagt de beheerder zorg voor een evenwichtige samenstelling van het college, waarbij geen enkele partij overheerst. Hiertoe beoordeelt de beheerder periodiek en ten minste éénmaal per jaar het draagvlak in en de samenstelling van het CCvD.

De benoeming van de leden, alsmede van de voorzitter, van het CCvD geschiedt volgens een daartoe op te stellen procedure. De voorzitter en de leden hebben zitting gedurende 5 jaar. Een lid of de voorzitter treedt af wanneer tenminste één van de omstandigheden voordoet zoals vermeld in genoemde procedure. Het CCvD benoemt zelf een plaatsvervangend voorzitter uit haar midden.

Taken en verantwoordelijkheden
Het CCvD voorziet de beheerder gevraagd en ongevraagd van schriftelijk advies dat gericht is op het zo goed mogelijk laten functioneren van de Gedragscode. Adviezen kunnen onder andere zien op de volgende aspecten:

- De aard en de inhoud van de Gedragscode.
- Een aanleiding om de Gedragscode te wijzigen.
- De beoordelingscriteria die door de beheerder worden vastgesteld en door het toezichthoudend orgaan worden gebruikt.
- De omvang, zwaarte, frequentie en rapportage van de (initiële) audits.
- De eisen die gesteld worden aan de auditors.
- De wijze waarop het toezichthoudend orgaan aan de beheerder en het CCvD rapporteert.
- De vragen of adviezen van het toezichthoudend orgaan.
- Het gebruik en de betekenis van het logo als bewijs van deelname aan de Gedragscode.

Werkwijze
Het CCvD vergadert zo vaak als nodig is voor het goed functioneren van het college. Het CCvD vergadert minimaal éénmaal per jaar. Het CCvD neemt beslissingen met een volstrekte meerderheid van stemmen, uitgebracht door minimaal 50 procent van het aantal stemgerechtigde leden. De stemgerechtigde leden staan vermeld in de ledenregistratie van de

beheerder. Tenzij door de beheerder anders wordt bepaald, is ook de voorzitter stemgerechtigd.

Indien het vereiste percentage stemgerechtigde leden niet vertegenwoordigd is bij het nemen van het besluit, vindt een nieuwe bijeenroeping plaats. Besluiten die worden genomen bij deze nieuwe bijeenroeping, vinden plaats bij volstrekte meerderheid van stemmen ongeacht of voldaan wordt aan het eerder genoemde quorum.

Bij staken van stemmen beslist de voorzitter; indien de voorzitter afwezig is wordt het besluit aangehouden. De plaatsvervangend voorzitter heeft derhalve geen doorslaggevende stem. Indien het aantal stemmen tegen een te nemen besluit meer bedraagt dan 20 procent van het aantal geldig uitgebrachte stemmen, kan de minderheid verzoeken het belangrijkste minderheidsstandpunt in het verslag van de vergadering te laten opnemen.

Overigens regelt het CCvD zelfstandig haar werkwijze met inachtneming van het bepaalde in dit reglement.

Deskundigen
Het CCvD kan deskundigen op een specifiek gebied uitnodigen om één of meer vergaderingen bij te wonen. Deze personen zijn adviseur en hebben géén stemrecht.

Permanente commissie
Als het CCvD een permanente commissie wil instellen, legt zij dit vooraf ter goedkeuring voor aan de beheerder. Samenstelling, taak en werkwijze van een dergelijke commissie worden door de beheerder op voorstel van het CCvD schriftelijk bepaald en vastgesteld.

Openbaarheid en geheimhouding
De leden van het CCvD zullen bij de uitvoering van hun werkzaamheden strikte geheimhouding betrachten tegenover derden, zowel tijdens als ook na beëindiging van hun lidmaatschap, omtrent alle informatie en gegevens die hen ter kennis komen in het kader van het lidmaatschap van het CCvD. Zij ondertekenen daartoe een geheimhoudingsverklaring.

20.3 Toezichthoudend orgaan (EBN Certification)

Op verzoek van de beheerder van de Gedragscode heeft de AP EBN Certification geaccrediteerd om als extern en onafhankelijk toezichthoudend orgaan voor de gedragscode te fungeren (zie bijlage 17).

Onafhankelijk, deskundig en geaccrediteerd
Het toezichthoudend orgaan is onafhankelijk en deskundig met betrekking tot het onderwerp van de Gedragscode en heeft transparante en toegankelijke procedures vastgesteld. Ter bevestiging daarvan is het toezichthoudend orgaan door de AP geaccrediteerd.

Taken
Het is de taak van het toezichthoudend orgaan om:

- te beoordelen of een ISPS-bedrijf aan de beoordelingscriteria van de Gedragscode voldoet;
- toezicht te houden op de naleving van de Gedragscode;
- periodiek te toetsen of de Gedragscode goed functioneert;
- klachten te behandelen over inbreuken op de Gedragscode of over de wijze waarop aan de Gedragscode uitvoering wordt gegeven.

20.4 Deelnemen

ISPS bedrijven die willen deelnemen aan de Gedragscode dienen daarvoor een verzoek in te dienen bij de beheerder. De beheerder meldt de beoogde nieuwe deelnemer aan bij het toezichthoudend orgaan die vervolgens een audit uitvoert. Wanneer deze audit naar behoren is volbracht wordt het ISPS bedrijf als deelnemer geregistreerd en als zodanig aangemeld bij de AP.

Contactgegevens

Port Privacy B.V.

Contactpersoon	De heer T.H. Poot
Adres	Nieuwe Sluisstraat 4a, 3111 PJ Schiedam
Website	www.portprivacy.com
Telefoonnummer	0624751388
Emailadres	info@portprivacy.com

Centraal College van Deskundigen

Contactpersoon	nnb
Adres	nnb
Telefoonnummer	nnb
Emailadres	nnb

EBN Certification B.V.

Contactpersoon	De heer C. van Zwienen
Adres	Heliotroopring 1100, 3316 KG Dordrecht
Website	www.ebncertification.nl
Telefoonnummer	0782003400
Emailadres	info@ebncertification.nl

Bijlage 1 - Verzoek tot goedkeuring van de Gedragscode

Verzoekschrift
Hierbij verzoekt Port Privacy B.V. (Port Privacy) de Nederlandse Autoriteit Persoonsgegevens om de onderhavige en bijgaande Gedragscode goed te keuren voor de duur van 5 jaar. Het verzoek is gebaseerd op artikel 40 AVG en betreft de Privacy gedragscode voor het toegangsbeleid van ISPS-bedrijven in Nederland.

Dit verzoek wordt tegelijkertijd in gediend met het verzoek ex artikel 41 lid 2 AVG tot de accreditatie van EBN Certification B.V. ten behoeve van het toezicht op de naleving van de Gedragscode (zie bijlage 16 van de Gedragscode).

Datum verzoek
Het verzoek is ingediend op 17 september 2019.

Verzoeker
Het verzoek wordt gedaan door Port Privacy.

Contactpersoon	Tjeerd Poot
Adres	Nieuwe Sluisstraat 4a, 3111 PJ Schiedam
Website	www.portprivacy.com
Telefoonnummer	0624751388
Emailadres	tjeerdpoot@portprivacy.com

Werkgroep
De Gedragscode is opgesteld door Port Privacy in samenwerking met de Werkgroep. De Werkgroep bestaat uit een aantal ISPS/AEO-bedrijven en een aantal andere belanghebbenden.

Verwerkingsverantwoordelijke ISPS/AEO-bedrijven die lid zijn van de Werkgroep:
- APM Maasvlakte II B.V.
- APM Terminal Rotterdam B.V.
- European Bulk Services B.V.
- Europees Massagoed Overslagbedrijf B.V.
- Gate Terminal B.V.
- Huntsman Holland B.V.
- Hutchison Ports ECT Rotterdam B.V.
- Kramer Group B.V.
- Rotterdam World Gateway B.V.

Andere belanghebbenden die lid zijn van de Werkgroep:
- Belastingdienst Douane
- by DnA
- Havenbedrijf Rotterdam N.V.
- Royal Dirkzwager B.V.
- Secure Logistics B.V.
- Securitas Rotterdam B.V.

- Vereniging Deltalinqs
- Zeehavenpolitie

Vertegenwoordiging
Port Privacy vertegenwoordigt de Werkgroep. Dit blijkt uit de brieven in bijlage V1. De daarin ondertekende verklaringen luiden telkens:

> *Hierbij verklaar ik dat [bedrijfsnaam] lid is van de in deze brief bedoelde Werkgroep, de Werkgroep representatief is voor de sector van ISPS-bedrijven, Port Privacy de Werkgroep vertegenwoordigt in het project om te komen tot een of meer privacy gedragscodes voor het toegangsbeleid van Nederlandse ISPS-bedrijven en Port Privacy de Werkgroep dus vertegenwoordigt in haar communicatie en procedures met de Autoriteit Persoonsgegevens, o.a. in de goedkeuringsprocedure ex artikel 40 AVG.*

Bevoegde Toezichthoudende Autoriteit
Het verzoek is gericht aan en ingediend bij de Nederlandse Autoriteit Persoonsgegevens (AP). De AP is bevoegd om deze Gedragscode te beoordelen en goed te keuren omdat de verwerkingsactiviteiten waar de Gedragscode op ziet plaatsvinden in Nederland en ook de verwerkingsverantwoordelijken en de betrokkenen zich in Nederland bevinden, evenals de hoofdvestiging van Port Privacy en het toezichthoudend orgaan.

Onderbouwing van het verzoek
Ter onderbouwing van het verzoek wordt volstaan met een verwijzing naar de Gedragscode en de antwoorden op de checklist die hieronder uit de Guidelines is overgenomen.

<u>Heeft u een toelichting en alle relevante ondersteunende documentatie verstrekt?</u>
Ja. Zie de leeswijzer in hoofdstuk 1 en voorts alle bijlagen van de Gedragscode.

<u>Bent u een organisatie die categorieën van controllers of processors vertegenwoordigt?</u>
Ja. Zie hoofdstuk 5 van de Gedragscode, alsmede bijlage V1 bij dit verzoekschrift.

<u>Heeft u gegevens verstrekt om aan te tonen dat u een effectief representatief orgaan bent dat in staat is om de behoeften van uw leden te begrijpen?</u>
Ja. Zie hoofdstuk 5 van de Gedragscode, alsmede bijlage V1 bij dit verzoekschrift.

<u>Heeft u de verwerkingsactiviteiten en de verwerkingsproblemen duidelijk gedefinieerd?</u>
Ja. Zie hoofdstuk 6 en de hoofdstukken 7 t/m 18 van de Gedragscode.

<u>Heeft u de territoriale reikwijdte bepaald en, indien relevant, een lijst van alle betrokken toezichthoudende autoriteiten opgesteld?</u>
Ja. Zie hoofdstuk 2 van de Gedragscode.

<u>Hebt u verantwoord waarom de Nederlandse Autoriteit Persoonsgegevens bevoegd is?</u>
Ja, in de vorige paragraaf van dit verzoekschrift.

Hebt u mechanismen opgenomen die een effectieve controle mogelijk maken van de naleving van de code?
Ja. Zie paragraaf 20.3 van de Gedragscode.

Hebt u een toezichtsorgaan geïdentificeerd en uitgelegd hoe die het toezicht zal vormgeven?
Ja. Zie paragraaf 20.3 van de Gedragscode.

Hebt u informatie opgenomen over de mate van raadpleging die is uitgevoerd bij de ontwikkeling van het code?
Ja. Zie bijlage 4 van de Gedragscode.

Hebt u, waar relevant, bevestigd dat de conceptcode in overeenstemming is met de wetgeving(en) van de lidstaten?
Ja. De Gedragscode zoals deze wordt ingediend op 17 september 2019 is in overeenstemming met de in Nederland geldende wetgeving. Zie ook paragraaf 6.8 van de Gedragscode.

Wordt aan de taalvereisten voldaan?
Ja. Zie hoofdstuk 1 van de Gedragscode.

Bevat uw inzending voldoende details om aan te tonen dat de AVG juist wordt toegepast?
Ja. De Gedragscode beslaat alle aspecten van de AVG die aan de orde zijn bij verwerkingen in het kader van het toegangsbeleid van ISPS/AEO-bedrijven. De verwerkingen worden gedetailleerd beschreven en per categorie van betrokkenen volledig verantwoord.

Toelichting
Uiteraard is Port Privacy graag bereid om haar verzoek mondeling en/of met stukken, nader te onderbouwen en/of toe te lichten.

Conclusie en verzoek
Port Privacy komt tot de conclusie dat de Gedragscode voldoet aan de eisen die de AVG en de Guidelines daar aan stellen en verzoekt de AP dan ook om de Privacy Gedragscode voor het toegangsbeleid van ISPS-bedrijven voor de duur van 5 jaar goed te keuren.

Ondertekening

Schiedam, 17 september 2019

_____
Port Privacy B.V.
mr. T.H. Poot

Bijlage 2 - Goedkeuringsverklaring

Toevoegen na ontvangst van de goedkeuring

Bijlage 3 - Verwijzingsstabel Guidelines en Gedragscode

In de Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (adopted on 12 februari 2019, version for public consultation) zijn richtlijnen opgenomen die zien op de ontvankelijkheid in een goedkeuringsprocedure ex artikel 40 (H5, Admissibility of a draft code) en op criteria voor goedkeuring (H6, Criteria for approving codes).

Uit onderstaande tabel volgt waar de verschillende bepalingen uit de Guidelines in de Gedragscode zijn verwerkt.

Guidelines	Onderwerp	Gedragscode
5.1	Toelichting	H1
5.2	Representativiteit en vertegenwoordiging	H5, Bijlage V1
5.3	Materiële reikwijdte	H2
5.4	Territoriale reikwijdte	H2
5.5	Bevoegdheid AP	Bijlage 1
5.6	Mechanisme voor toezicht	H20, Bijlagen V2 t/m V9
5.7	Toezichthoudend orgaan	H20, Bijlagen V2 t/m V9
5.8	Raadpleging belanghebbenden	Bijlage 4
5.9	Nationale wetgeving	H1
5.10	Taal	H1
5.11	Checklist	Bijlage 1
6.1	Specifieke behoefte	H1, H6 en H7 t/m H18
6.2	Vergemakkelijking van effectieve toepassing AVG	H6 en H7 t/m H18
6.3	Specificering van toepassing AVG	H6 en H7 t/m H18
6.4	Mechanismen voor effectief toezicht	H20, Bijlagen V2 t/m V9

Bijlage 4 - Totstandkoming gedragscode

Inleiding
De gedragscode is opgesteld en bij de AP ter goedkeuring ingediend door Port Privacy in samenwerking met de Werkgroep.

Samenstelling Werkgroep
De Werkgroep bestaat uit een aantal ISPS-bedrijven en een aantal andere belanghebbende organisaties. Zij vormen een goede dwarsdoorsnede van de (maritieme) sector: ISPS-bedrijven zijn gehouden aan de ISPS Code. Daartoe schakelen zij Havenbeveiligingsbedrijven in, zoals Securitas. Logistieke platforms, zoals het platform van Dirkzwager, maken een efficiënte en effectieve uitvoering van het toegangsbeleid mogelijk. Datzelfde geldt voor de leveranciers van toegangsmanagementsystemen, zoals Secure Logistics. Havenbedrijven, zoals het Havenbedrijf Rotterdam, heeft tot taak om de naleving van de ISPS te controleren. De Douane richt zich op de goederenstroom en de Zeehavenpolitie bestrijdt de criminaliteit waarbij onbevoegde toegang aan de orde is. Ondernemersverenigingen, zoals Deltalinqs, behartigen de belangen van bedrijven in de sector.

Rol Werkgroep
Alle leden zijn gevraagd om actief aan de Werkgroep deel te nemen en om de opstellers van de Gedragscode van informatie uit de praktijk te voorzien. Dit is ook daadwerkelijk gebeurd; in gesprekken, besprekingen en per mail. Behalve het leveren van input heeft de Werkgroep ook de taak gehad om feedback te leveren op conceptteksten voor de Gedragscode. Ook dit is in ruime mate aan de orde geweest.

Bijeenkomsten Werkgroep
De Werkgroep is sinds de zomer van 2017 12 maal bijeen gekomen (gemiddeld 1x per 2 maanden). De medewerkers van Port Privacy hebben in september 2017 een presentatie verzorgd voor de leden van de werkgroep. In deze presentatie is een introductie van de AVG gegeven en de veranderingen die de inwerkingtreding van deze wet met zich meebrengen voor de specifiek sector van ISPS bedrijven. Deze presentatie is vervolgens ter beschikking gesteld aan alle aanwezigen.

Hierna is er een checklist opgesteld welke door de werkgroepleden individueel is ingevuld. De beantwoording van deze checklist heeft als basis gediend voor gedragscode. Deze checklist is zo goed en gedetailleerd mogelijk door ieder lid van de werkgroep ingevuld zodat we alle mogelijke knelpunten in detail konden worden beoordeeld. Op deze wijze is er geïnventariseerd hoe het toegangsbeleid thans wordt uitgevoerd. Gebleken is dat dit in de hele sector onderling weinig van elkaar verschilt. Vervolgens is onderzocht of en waar de huidige praktijk knelt met de (nieuwe) privacyregels. Daar waar knellingen werden geconstateerd, is bedacht hoe het toegangsbeleid kan worden aangepast zodat alsnog wordt voldaan aan de AVG. Het aldus gewijzigde toegangsbeleid is vervolgens nogmaals beoordeeld aan de hand van alle eisen die volgen uit de AVG en tot slot, nadat is geconstateerd dat aan alles wordt voldaan, verwerkt in de Gedragscode.

In de navolgende bijeenkomsten is er telkens aan de hand van een vastgestelde agenda met de leden van de Werkgroep gesproken over de inhoudelijke voortgang van de ontwikkeling van de gedragscode. Tijdens deze bijeenkomsten zijn alle bevindingen en conceptteksten met de Werkgroep besproken. Ook is er regelmatig per mail en per telefoon met elkaar overlegd.

Raadpleging verwerkingsverantwoordelijke ISPS-bedrijven
De ISPS-bedrijven die lid zijn van de werkgroep zijn representatief voor de sector van ISPS-bedrijven. Verwezen wordt naar hoofdstuk 5 van de Gedragscode. Door de Gedragscode te ontwikkelen in nauwe, intensieve samenwerking met de Werkgroep is er sprake van een passend niveau van raadpleging van de verwerkingsverantwoordelijken.

Raadpleging overige belanghebbenden
Alle overige belanghebbenden (Havenbedrijven, Beveiligingsbedrijven, Belastingdienst Douane, Zeehavenpolitie en Ondernemersverenigingen) zijn vertegenwoordigd in de Werkgroep. Door de Gedragscode te ontwikkelen in nauwe samenwerking met de Werkgroep is er sprake van een passend niveau van raadpleging van de overige belanghebbenden. Daarnaast heeft Port Privacy in 2017 en 2018 diverse presentaties voor overige belanghebbenden over het tot stand komen en ontwikkelen van de Gedragscode voor deze specifieke sector verzorgd. Er hebben presentaties plaatsgevonden bij:

- Port of Moerdijk
- ORAM Ondernemend Amsterdam
- Landelijk Overleg Port Security (LOPS)
- ASIS Security Congres
- Deltalinqs
- Security Advies Platform
- ISC Port Safety & Security

Raadpleging betrokkenen
Ook betrokkenen hebben belang bij de Gedragscode. In de Gedragscode worden meerdere categorieën van betrokkenen onderscheiden. Port Privacy heeft zich ingespannen om de standpunten van deze categorieën te achterhalen en in de Gedragscode te verwerken.

Categorie van betrokkenen	Vertegenwoordigende organisaties
Scheepsbemanning	VRC
Werknemers	OR's van ISPS-bedrijven die lid zijn van de Werkgroep
Externe arbeidskrachten	VOMI
Leveranciers en shipchandlers	NVVS
Bootmannen en sjorders	KRVE en ILS Matrans
Vrachtautochauffeurs	TLN
Binnenvaartbemanning	BLN Schuttevaer
Vrachttreinpersoneel	DB Cargo
Overheidspersoneel	n.v.t. (vertegenwoordigd in Werkgroep)
Bezoekers	n.v.t.
Onbevoegden	n.v.t.
Kinderen	BLN Schuttevaer

Dit is gebeurd door diverse vertegenwoordigende organisaties of marktleiders aan te schrijven, na te bellen en, in sommige gevallen, te bezoeken en te interviewen. De standpunten van de betrokkenen zijn, waar mogelijk en indien van toepassing, verwerkt in de Gedragscode.

Na een korte uitleg van het voornemen de Gedragscode op te stellen en de rol van betrokkenen in het toegangsbeleid, zijn de genoemde organisaties concreet de navolgende vragen gesteld:

- Hoe wordt het huidige toegangsbeleid van havenbedrijven ervaren als het gaat om de privacy?
- Hoe kan het toegangsbeleid op het gebied van privacy worden verbeterd?
- Hoe kunnen wij zo goed mogelijk rekening houden met de privacybelangen van uw leden?
- Wat vindt men van een sectorbrede privacy gedragscode voor ISPS-bedrijven?
- Heeft u overige vragen of opmerkingen?

Beoordeling en akkoord
De finale versie is door alle leden van de Werkgroep beoordeeld en akkoord bevonden. Tot slot is de Gedragscode ter goedkeuring bij de AP ingediend.

Bijlage 5 - Definities

Algemene Verordening Gegevensbescherming (AVG)
De Algemene Verordening Gegevensbescherming (2016/679) is de privacy verordening die sinds 25 mei 2018 voor elk lidstaat van de Europese Economische Ruimte van toepassing is. De AVG bevat regels voor de verwerking van persoonsgegevens.

Authorised Economic Operator (AEO)
Een Authorised Economic Operator, of geautoriseerde marktdeelnemer, is de naam voor een status voor internationaal opererende bedrijven. Deze status wordt verkregen middels een vergunning die wordt afgegeven door de Belastingdienst Douane wanneer aan de criteria wordt voldaan. Deze criteria zien met name op de internationale veiligheid van de vervoersketen en zijn opgenomen in het communautair douanewetboek (925/2013) en de bijpassende toepassingsverordeningen. Een AEO-vergunning biedt bedrijven voordelen in het internationale handelsverkeer. Zo wordt er minder streng gecontroleerd bij grensoverschrijdende handel met als gevolg dat er minder oponthoud is bij het passeren van de grenzen.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens is het onafhankelijke orgaan dat toezicht houdt op naleving van de AVG. Het is bevoegd tot handhaving middels onderzoek en het geven van waarschuwingen, terechtwijzingen, bevelen, beperkingen, verboden, opschortingsmaatregelen en boetes met een maximum van 20 miljoen of 4% van de wereldwijde omzet per overtreding.

Betrokkene
De ‘natuurlijk persoon’ zoals bedoeld is in de definitie van persoonsgegevens. In deze gedragscode worden meerdere categorieën van betrokkenen onderscheiden.

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn:

- gegevens waaruit ras of etnische afkomst blijkt;
- gegevens waaruit politieke opvattingen blijken;
- gegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- gegevens waaruit het lidmaatschap van een vakbond blijkt;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Binnenvaartschip
Een schip dat vaart op binnenwateren, niet zijnde een ‘zeeschip’. Een binnenvaartschip valt niet onder de ISPS Code.

Biometrische gegevens
Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk

persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

Burgerservicenummer (BSN)
Het unieke nationaal identificatienummer zoals dat door Nederland aan natuurlijke personen wordt verstrekt.

Company Security Officer (CSO)
De functionaris die werkzaam is voor een rederij en verantwoordelijk is voor het voldoen aan de eisen die volgen uit de ISPS Code. Wordt deze functionaris in de Gedragscode wordt genoemd, dan refereert dit zowel aan de functionaris als aan degenen aan wie diens bevoegdheden zijn gedelegeerd.

Datalek
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Digitaal informatieplatform over actuele scheepsbewegingen
Een digitaal platform waarop actuele informatie wordt verstrekt over scheepsbewegingen met o.a. de verwachte aankomsttijden van schepen in havens over de hele wereld. Via het platform kunnen aanmeldingen worden verricht van schepen en betrokkenen zoals de scheepsbemanning, leveranciers, shipchandlers en bezoekers.

European Data Protection Board
Zie ‘WP29 / European Data Protection Board’.

Europese Economische Ruimte (EER)
Alle lidstaten van de Europese Unie plus Liechtenstein, Noorwegen en IJsland.

Gedragscode
De onderhavige gedragscode.

Guidelines
De EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (adopted on 12 february 2019, version for public consultation).

Havenbeveiligingsbedrijf
Een havenbeveiligingsbedrijf dat wordt ingeschakeld door een ISPS-bedrijf om uitvoering te geven aan het beveiligings- en veiligheidsbeleid en dus ook het toegangscontrolebeleid. Een beveiligingsbedrijf valt onder de wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr). Deze wet bevat regels over het bewaken van de veiligheid van personen en goederen of het waken tegen verstoring van de orde en rust op terreinen en in gebouwen. Het verrichten van deze werkzaamheden is louter toegestaan op grond van een vergunning. Een

havenbeveiligingsbedrijf werkt louter met beveiligers die een havenbeveiligingscertificaat hebben conform de Havenbeveiligingswet.

Havenbeveiligingswet
De Havenbeveiligingswet geeft uitvoering aan de verordening waarin de ISPS Code is opgenomen (725/2004).

Havenbeheersverordening
De verordening van de gemeente Rotterdam waarin noodzakelijke regels zijn opgenomen ter bevordering van een goed havenbeheer (2010, versie januari 2016).

ID-nummer
Een ID-nummer betreft het document/kaart-nummer van een identiteitsbewijs.

International Ship and Port facility Security Code (ISPS Code)
De internationale code voor de beveiliging van schepen en havenfaciliteiten (International Ship and Port facility Security Code, ISPS Code) is een amendement van 12 december 2002 op het Verdrag voor beveiliging van mensenlevens op zee (SOLAS) waarin de minimumeisen in verband met de beveiliging van schepen, havenfaciliteiten en overheidsinstellingen beschreven staan. De code trad in werking op 31 maart 2004 met de Europese verordening 725/2004 en beschrijft de verantwoordelijkheden van overheden, rederijen, personeel aan boord van schepen en personeel van havenfaciliteiten in verband met het detecteren van bedreiging van de veiligheid en het nemen van preventieve maatregelen om incidenten omtrent beveiliging te voorkomen, die een bedreiging vormen voor schepen en havenfaciliteiten betrokken in de internationale handel.

ISPS-bedrijf
Een bedrijf dat is gericht op de internationale handel, waar internationaal scheepvaartverkeer wordt afgehandeld en dat gecertificeerd is voor de ISPS-regelgeving. Voor een exacte definitie wordt verwezen naar Voorschriften 1 en 2 van Bijlage I van EU 725/2004.

Lading
Met lading wordt in deze gedragscode bedoeld alles dat wat door schepen, vrachtauto's, binnenvaartschepen en vrachttreinen wordt vervoerd, zoals containers, bulkgoederen, chemische vloeistoffen, enz.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, waarbij als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

Port Facility Security Officer (PFSO)
Functionaris werkzaam voor een ISPS-bedrijf en verantwoordelijk voor het voldoen aan de eisen die volgen uit de ISPS Code. Wanneer deze functionaris in de Gedragscode wordt

genoemd, refereert dit aan de functionaris zelf en/of op degenen aan wie zijn bevoegdheden zijn gedelegeerd.

Port Facility Security Plan (PFSP)
Het beveiligingsplan van het ISPS-bedrijf. In dit plan worden de beveiligings- en veiligheidsmaatregelen beschreven door het ISPS-bedrijf zijn genomen, zoals het toegangscontrolebeleid, waaronder het gebruik van beveiligingscamera's. Het plan wordt goedgekeurd door de PSO. Het plan geeft aan welke organisatorische, bouwkundige en elektronische beveiligingsmaatregelen zijn getroffen. In het plan zijn aan alle functies binnen het bedrijf eigen toegangsprofielen toegekend.

Port Security Officer (PSO)
De functionaris die, op basis van mandatering door de burgermeester, werkzaam is voor het semi-overheidsorgaan dat onder meer verantwoordelijk is voor het toetsen en goedkeuren van PFSP's, het afgeven van havenbeveiligingscertificaten en het houden van toezicht op ISPS-bedrijven. Wanneer deze functionaris in de Gedragscode wordt genoemd, refereert dit aan de functionaris zelf en/of op degenen aan wie zijn bevoegdheden zijn gedelegeerd.

Schip
Zeeschepen op internationale reizen, inclusief passagiersschepen, cargoschepen van 500 GT of hoger en offshore boorplatformen; niet zijnde een binnenvaartschip.

Ship Security Officer (SSO)
Functionaris werkzaam voor en op een schip en verantwoordelijk voor het voldoen aan de eisen die volgen uit de ISPS Code. Wanneer deze functionaris in de Gedragscode wordt genoemd, refereert dit aan de functionaris zelf en/of op degenen aan wie zijn bevoegdheden zijn gedelegeerd.

Terminal
Een andere naam voor het gehele of een deel van een ISPS-bedrijf.

Toegangsprofiel
Een toegangsprofiel geeft aan welke delen van het ISPS-bedrijf toegankelijk zijn en welke delen niet mogen worden betreden. In het PFSP wordt aan elke functie binnen het ISPS-bedrijf een toegangsprofiel toegekend.

Werkgroep
De werkgroep betreft de groep van organisaties met wie Port Privacy de Gedragscode heeft ontwikkeld. Verwezen wordt naar het verzoekschrift tot goedkeuring van de Gedragscode.

Verwerker
Een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dat persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke.

Verwerking
Een verwerking of een geheel van verwerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op een andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke
Een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dat, alleen of samen met andere bedrijven, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

WP29 / European Data Protection Board (EDPB)
De ‘Artikel 29 Werkgroep’ (WP29) is een adviesorgaan dat gezaghebbende opinies afgeeft omtrent privacyvraagstukken. Met ingang van 25 mei 2018 wordt de WP29 opgenomen in de European Data Protection Board: het Europese hoofdorgaan waar alle nationale Autoriteiten Persoonsgegevens lid van zijn.

PORT PRIVACY

Bijlage 6 - Beschrijving sector

ISPS-bedrijven
ISPS-bedrijven zijn op de internationale handel gerichte bedrijven waar internationaal scheepvaartverkeer wordt afgehandeld. Er zijn 4 subcategorieën te onderscheiden: Bulk, Chemische industrie, Containerterminals en Empty depots. Voor deze havengerelateerde bedrijven is het verplicht om zich te certificeren voor de International Ship and Port Facility Security Code (ISPS Code).

ISPS Code
De International Ship and Port facility Security Code is een amendement op het Verdrag voor beveiliging van mensenlevens op zee (SOLAS) naar aanleiding van de aanslagen op 11 september 2001. De ISPS Code is overgenomen in de Europese verordening 725/2004. Naast de ISPS Code geldt ter nadere uitvoering daarvan, de Havenbeveiligingswet.

De ISPS Code ziet op de veiligheid en beveiliging van schepen en havenfaciliteiten door een vroegtijdige verzameling en uitwisseling van informatie op veiligheidsgebied. Het doel is om burgers en milieu te beschermen tegen het gevaar van opzettelijke ongeoorloofde acties zoals terrorisme, piraterij of vergelijkbare acties zoals drugssmokkel. De ISPS Code zorgt er voor dat dit op een homogene wijze geschiedt. De ISPS Code beoogt voorts een basis te leggen voor een geharmoniseerde interpretatie en implementatie van de communautaire controle op de speciale maatregelen ter verbetering van de veiligheid. Meer in het bijzonder is het doel van de code om te zorgen voor een vroegtijdige en doeltreffende verzameling en uitwisseling van informatie op veiligheidsgebied.

Belang voor Nederland
Met de invoering van de ISPS Code heeft de maritieme sector een beveiligingsregime gekregen dat globaal hetzelfde gewicht heeft als het beveiligingsregime in de luchtvaart.

De ratio is dat het mondiale karakter van de sector, gevoegd bij de vitale functie die deze heeft voor de wereldeconomie (meer dan 90% van de wereldhandel gaat over zee), een mate van kwetsbaarheid heeft die de maatregelen wettigt.

Als logistiek centrum (Gateway) van Europa vervult Nederland, met Rotterdam als wereldhaven, een spilfunctie in de overzeese handel.

Deze spilfunctie is niet alleen van wezenlijk belang voor de Nederlandse economie, maar ook voor een aanzienlijk gedeelte van het Europese achterland. Nederland is derhalve gebaat bij een goed beveiligde vervoersketen. Dit zowel om schade door aanslagen te voorkomen, als om een betrouwbare politieke-, handels-, en vervoerspartner te zijn en te blijven voor andere landen. In dit laatste verband is beveiliging een wezenlijke factor in de internationale concurrentieverhoudingen geworden.

Daarnaast is voor de Nederlandse positie van belang het feit dat een aanmerkelijk deel van de VS olie-importen uit Nederland komt en dat de Rotterdamse regio het centrum is van de Europese strategische olievoorraden. Een hoog beveiligingsniveau brengt kwaliteit en aldus continuïteit en groei van de vervoersstromen en levert bovendien een bijdrage aan het Nederlandse beleid op het gebied van criminaliteitsbestrijding.

Bijlage 7 - Arbeidsomstandighedenwet

Algemeen
De Arbeidsomstandighedenwet ziet op de veiligheid en gezondheid van werknemers en derden.

Artikel 3 lid 1 sub e
De werkgever zorgt voor de veiligheid en de gezondheid van de werknemers inzake alle met de arbeid verbonden aspecten en voert daartoe een beleid dat is gericht op zo goed mogelijke arbeidsomstandigheden, waarbij hij, gelet op de stand van de wetenschap en professionele dienstverlening, het volgende in acht neemt: (…) e) doeltreffende maatregelen worden getroffen op het gebied van de eerste hulp bij ongevallen, de brandbestrijding en de evacuatie van werknemers en andere aanwezige personen, en doeltreffende verbindingen worden onderhouden met de desbetreffende externe hulpverleningsorganisaties.

Uit dit artikel volgt dat een werkgever dient te zorgen voor de veiligheid en de gezondheid van haar werknemers inzake alle met de arbeid verbonden aspecten. Zij dient daartoe een beleid te voeren dat is gericht op zo goed mogelijke arbeidsomstandigheden, o.a. op het gebied van de eerste hulp bij ongevallen, brandbestrijding, evacuatie en verbindingen met externe hulpverleningsorganisaties. Uit artikel 10 (zie ook verderop) en uit de rechtspraak volgt dat de arbeidsomstandighedenwet ook geldt voor externe arbeidskrachten en anderen die zich op de werkvloer van de werkgever (het terrein) bevinden.

Artikel 6
De werkgever neemt bij het voeren van het arbeidsomstandighedenbeleid de maatregelen die nodig zijn ter voorkoming en beperking van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken en de gevolgen daarvan voor de veiligheid en de gezondheid van de in het bedrijf, de inrichting, of een deel daarvan werkzame werknemers. Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot:

a) de categorieën van bedrijven, inrichtingen of delen daarvan ten aanzien waarvan de werkgever die maatregelen neemt;
b) de gegevens die de werkgever met betrekking tot de bedrijven, inrichtingen of delen daarvan, bedoeld onder a, op schrift stelt of verstrekt aan de toezichthouder of aan de werknemers en de andere deskundige personen, bedoeld in artikel 13, eerste tot en met derde lid, de personen, bedoeld in artikel 14, eerste lid en de arbodienst;
c) de maatregelen die de werkgever neemt ten aanzien van de bedrijven, inrichtingen of delen daarvan, bedoeld onder a;
d) het tijdstip waarop en de frequentie waarmee wordt voldaan aan de verplichtingen, bedoeld onder b en c;
e) een verbod op de exploitatie van het bedrijf, de inrichting of een deel daarvan, indien niet of niet voldoende is voldaan aan een of meer verplichtingen krachtens dit artikel;
f) het toezicht op de naleving van het bij of krachtens dit artikel bepaalde.

Uit dit artikel volgt dat een werkgever bij het voeren van het arbeidsomstandighedenbeleid de maatregelen moet nemen die nodig zijn ter voorkoming en beperking van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken. Een deel van de ISPS-bedrijven zijn ook BRZO-

bedrijven; bedrijven waar gevaarlijke stoffen worden verwerkt en waarvoor het Besluit Risico's Zware Ongevallen van toepassing is.

Artikel 10
Indien bij of in rechtstreeks verband met de arbeid die de werkgever door zijn werknemers doet verrichten in een bedrijf of een inrichting of in de onmiddellijke omgeving daarvan gevaar kan ontstaan voor de veiligheid of de gezondheid van andere personen dan die werknemers, neemt de werkgever doeltreffende maatregelen ter voorkoming van dat gevaar.

Uit dit artikel volgt dat een werkgever ook maatregelen moet nemen ter voorkoming van gevaar voor de veiligheid en gezondheid van andere personen dan zijn werknemers. Eén van de maatregelen is om er voor te zorgen dat bij een incident snel duidelijk is wie er zich op het terrein bevinden.

Artikel 15 lid 1
De werkgever laat zich ten aanzien van de naleving van zijn verplichtingen op grond van artikel 3, eerste lid, onder e, van deze wet bijstaan door een of meer werknemers die door hem zijn aangewezen als bedrijfshulpverleners.

Uit dit artikel volgt dat een werkgever zich bij de verplichtingen uit hoofde van artikel 3 lid 1 sub e laat bijstaan door één of meer werknemers die zijn aangewezen als bedrijfshulpverleners.

Koppeling met de Gedragscode
Uit de bovenbeschreven regelgeving volgt dat het voor een ISPS-bedrijf noodzakelijk is om een beveiligings- en veiligheidsbeleid te voeren. Een noodzakelijk onderdeel daarvan is het toegangsbeleid. Bij een gedegen uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Een ISPS-bedrijf verwerkt dus persoonsgegevens bij het uitvoeren van cq. voldoen aan de in deze bijlage beschreven regelgeving.

Bijlage 8 - Authorised Economic Operator (AEO)

Algemeen
Een Authorised Economic Operator, of geautoriseerde marktdeelnemer, is de naam voor een status voor internationaal opererende bedrijven. Deze status wordt verkregen middels een vergunning die wordt afgegeven door de Belastingdienst Douane wanneer aan de criteria wordt voldaan. Deze criteria zien met name op de internationale veiligheid van de vervoersketen en zijn opgenomen in het communautair douanewetboek (925/2013) en de bijpassende toepassingsverordeningen. Een AEO-vergunning biedt bedrijven voordelen in het internationale handelsverkeer. Zo wordt er minder streng gecontroleerd bij grensoverschrijdende handel met als gevolg dat er minder oponthoud is bij het passeren van de grenzen.

Bedrijfseconomisch zijn de meeste ISPS-bedrijven genoodzaakt om in het bezit te zijn van een AEO-vergunning. De eisen die uit de AEO voortvloeien, zijn, ter zake van het toegangsbeleid, gelijk aan de eisen die voortvloeien uit de ISPS Code.

Titel 1, Hoofdstuk 2, Afdeling 4, artikel 39 sub e – 'verlenen van status'
De criteria voor de toekenning van de status van "geautoriseerde marktdeelnemer" zijn de volgende: (…) e) passende veiligheidsnormen waaraan geacht wordt voldaan te zijn als de aanvrager kan aantonen dat hij passende maatregelen handhaaft om de veiligheid van de internationale toeleveringsketen te waarborgen, onder andere op het gebied van de fysieke integriteit, toegangscontrole, logistieke processen, behandeling van specifieke soorten goederen, personeel en identificatie van zijn zakenpartners.'

Uit dit artikel volgt dat voor het verkrijgen van de AEO-status passende maatregelen moeten worden gehandhaafd om de veiligheid van de vervoersketen te waarborgen, onder andere op het gebied van het toegangsbeleid.

Koppeling met de Gedragscode
Uit de noodzaak om de veiligheid van de vervoersketen te waarborgen, onder andere op het gebied van het toegangsbeleid, volgt dat het voor een ISPS-bedrijf dat een AEO-vergunning heeft, noodzakelijk is om een beveiligings-, veiligheids- en toegangsbeleid te voeren. Bij een gedegen uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Een ISPS/AEO-bedrijf verwerkt dus persoonsgegevens bij het uitvoeren van cq. voldoen aan de in deze bijlage beschreven AEO-wetgeving.

Bijlage 9 - Besluit Risico Zware Ongevallen 2015

Artikel 5 lid 1
De exploitant treft alle maatregelen die nodig zijn om zware ongevallen te voorkomen en de gevolgen daarvan voor de menselijke gezondheid en het milieu te beperken.

Artikel 5 lid 2
De exploitant kan te allen tijde aantonen aan de aangewezen toezichthouders dat hij alle noodzakelijke maatregelen heeft getroffen.

Koppeling met de Gedragscode
Uit de bovenbeschreven regelgeving volgt dat het voor een ISPS-bedrijf noodzakelijk is om een beveiligings- en veiligheidsbeleid te voeren. Een noodzakelijk onderdeel daarvan is het toegangsbeleid. Bij een gedegen uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Een ISPS-bedrijf verwerkt dus persoonsgegevens bij het uitvoeren van cq. voldoen aan de in deze bijlage beschreven regelgeving.

PORT PRIVACY

Bijlage 10 - Havenbeheersverordening

Algemeen
In de Havenbeheersverordening Rotterdam 2010 zijn regels opgenomen met betrekking tot orde en gebruik in de haven, veiligheid en milieu, gevaarlijke stoffen, bunkeren, enzovoorts. In paragraaf 11 afdeling 2 en 4 staan regels over respectievelijk het vast- en losmaken van schepen door bootmannen en het sjorren van containers aan boord van schepen door sjorders.

Artikel 11.2.2 lid 2 en 3 en artikel 11.2.3 sub e
De bootman is tijdens de werkzaamheden voorzien van een geldig legitimatiebewijs, als bedoeld in artikel 11.2.3, onder e.

De bootman toont het legitimatiebewijs, bedoeld in artikel 11.2.3, onder e, op verzoek van personen of bedrijven die van zijn diensten gebruik maken.

Het college verleent een erkenning voor een bootliedenorganisatie, indien deze: (…) e) aan de bootlieden een legitimatiebewijs wordt verstrekt dat is voorzien van een goedgelijkende pasfoto en dat ten minste vermeldt:
1°. de naam, geboorteplaats en geboortedatum van de bootman;
2°. met goed gevolg de opleiding Bootman behaalt als bedoeld in artikel 11.2.2, eerste lid, onder a, met vermelding van datum van diplomaverstrekking, en;
3°. de naam van de bootliedenorganisatie waarbij de bootman is aangesloten.

Uit deze artikelen volgt dat een bootman tijdens zijn werkzaamheden moet zijn voorzien van een geldig legitimatiebewijs en dat dit legitimatiebewijs moet zijn voorzien van een goedgelijkende pasfoto en dat daarop ten minste moet worden vermeld de naam, geboorteplaats en geboortedatum van de bootman, dat de opleiding Bootman is behaald, de datum waarop het diploma is verstrekt en de naam van de bootliedenorganisatie waar de bootman bij is aangesloten.

Artikel 11.4.2 sub d en artikel 11.4.3 lid 3 en 4
Het college verleent een vergunning voor een sjorbedrijf, indien het sjorbedrijf: (…) d) aan de sjorders een legitimatiebewijs verstrekt dat is voorzien van een goedgelijkende pasfoto en dat ten minste vermeldt: 1°. de naam, geboorteplaats en geboortedatum van de sjorder, en; 2°. de naam van het sjorbedrijf waar de sjorder in dienst is.

De sjorder is tijdens de sjorwerkzaamheden voorzien van het legitimatiebewijs, bedoeld in artikel 11.4.2, onder d.

De sjorder toont het legitimatiebewijs, bedoeld in artikel 11.4.2, onder d, op verzoek van personen of bedrijven die van zijn diensten gebruik maken.

Uit deze artikelen volgt dat een sjorder tijdens zijn werkzaamheden moet zijn voorzien van een geldig legitimatiebewijs en dat dit legitimatiebewijs moet zijn voorzien van een goedgelijkende

pasfoto en dat daarop ten minste moet worden vermeld de naam, geboorteplaats en geboortedatum van de sjorder en de naam van het sjorderbedrijf waar de sjorder bij in dienst is.

Koppeling met de Gedragscode
Uit de bovenbeschreven regelgeving volgt dat het voor een ISPS-bedrijf noodzakelijk is om een beveiligings- en veiligheidsbeleid te voeren. Een noodzakelijk onderdeel daarvan is het toegangsbeleid. Bij een gedegen uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Een ISPS-bedrijf verwerkt dus persoonsgegevens bij het uitvoeren van cq. voldoen aan de in deze bijlage beschreven regelgeving.

PORT PRIVACY

Bijlage 11 - ISPS-Code (Verordening 2004/725)

Algemeen
De internationale code voor de beveiliging van schepen en havenfaciliteiten (International Ship and Port facility Security Code, ISPS Code) is een amendement van 12 december 2002 op het Verdrag voor beveiliging van mensenlevens op zee (SOLAS) waarin de minimumeisen in verband met de beveiliging van schepen, havenfaciliteiten en overheidsinstellingen beschreven staan.

De code trad in werking op 31 maart 2004 met de Europese verordening 725/2004 en beschrijft de verantwoordelijkheden van overheden, rederijen, personeel aan boord van schepen en personeel van havenfaciliteiten in verband met het detecteren van bedreiging van de veiligheid en het nemen van preventieve maatregelen om incidenten omtrent beveiliging te voorkomen, die een bedreiging vormen voor schepen en havenfaciliteiten betrokken in de internationale handel.

De inhoudsopgave van de verordening luidt als volgt:

Overwegingen verordening		1 t/m 17
Artikelen verordening		1 t/m 15
Bijlage I	voorschriften	1 t/m 13 (wijzigingen op SOLAS)
Bijlage II	Preambule	1 t/m 11 (ISPS-code)
Bijlage II	Deel A	1 t/m 19 (ISPS-Code)
Bijlage III	Deel B	1 t/m 19 (ISPS-Code)*

*) Over Deel B van Bijlage III stelt Overweging 8: ‘Deel B van de ISPS Code bevat enkele aanbevelingen waarvan de toepassing in de Gemeenschap verplicht dient te worden gesteld, om zo op homogene wijze te kunnen bijdragen tot verwezenlijking van de in de tweede overweging beschreven beveiligingsdoelstelling.’

Bijlage II, deel A, artikel 14 lid 2 – Veiligheid van de havenfaciliteit

Artikel 14.2
Bij veiligheidsniveau 1 dienen er in alle havenfaciliteiten in het kader van passende preventieve maatregelen tegen veiligheidsincidenten – rekening houdend met de richtsnoeren van deel B van deze Code – de volgende activiteiten te worden ondernomen: (…)

- zorgdragen voor de uitvoering van alle taken met betrekking tot de veiligheid van de havenfaciliteit;
- de toegang tot de havenfaciliteit controleren;
- bewaking van de havenfaciliteit, met inbegrip van anker- en aanlegplaats(en);
- bewaking van verboden terreinen, en zorgen dat allen bevoegd personeel toegang heeft
- toezicht op het laden en lossen van lading;
- toezicht op het laden en lossen van scheepsvoorraden, en
- zorgen dat er veiligheidscommunicatiemiddelen binnen handbereik zijn.

Bijlage II, deel A, artikel 16 lid 1 t/m 3 – Veiligheidsplan havenfaciliteit

Artikel 16.1
Voor iedere havenfaciliteit dient er op grond van een veiligheidsbeoordeling een veiligheidsplan te worden opgesteld en onderhouden dat toereikend is voor het schip/haven raakvlak. Het plan

dient bepalingen te bevatten voor de drie veiligheidsniveaus als gedefinieerd in dit Deel van de Code.

Artikel 16.1.1
Behoudens de bepalingen van paragraaf 16.2, mag een erkend beveiligingsbedrijf het veiligheidsplan voor een specifieke havenfaciliteit opstellen.

Artikel 16.2
Het havenfaciliteitveiligheidsplan dient te worden goedgekeurd door de verdragsluitende staat op wiens grondgebied de havenfaciliteit zich bevindt.

Artikel 16.3
Bij de ontwikkeling van een dergelijk plan wordt rekening gehouden met de richtsnoeren van Deel B van deze Code, en dit plan dient te worden gesteld in de werktaal of -talen van de havenfaciliteit. Het plan bevat ten minste de volgende onderdelen:

1. maatregelen om te voorkomen dat er voor gebruik tegen personen, schepen of havens bedoelde wapens of andere gevaarlijke stoffen en apparaten, waarvan het vervoer verboden is, de havenfaciliteit in of aan boord van een schip worden gebracht;
2. maatregelen om te voorkomen dat onbevoegden toegang krijgen tot de havenfaciliteit, tot in de havenfaciliteit aangemeerde schepen, en tot de verboden terreinen van de havenfaciliteit;
3. procedures waarmee kan worden gereageerd op veiligheidsbedreigingen of inbreuken op de veiligheid, met inbegrip van bepalingen inzake de handhaving van kritische operaties van de havenfaciliteit of het schip/haven raakvlak;
4. procedures waarmee kan worden gereageerd op eventuele veiligheidsinstructies die de verdragsluitende staat op wiens grondgebied de havenfaciliteit zich bevindt bij veiligheidsniveau 3 zou kunnen geven;
5. procedures voor evacuatie in geval van veiligheidsdreigingen of inbreuken op de veiligheid;
6. de taken van voor de beveiliging verantwoordelijk personeel van de havenfaciliteit en van ander personeel van de faciliteit in verband met beveiligingsaspecten;
7. procedures voor interfacing met de beveiligingsactiviteiten op het schip;
8. procedures voor periodieke beoordeling en bijwerking van het plan;
9. procedures voor het melden van veiligheidsincidenten;
10. identificatie van de veiligheidsbeambte van de havenfaciliteit, vergezeld van 24-uurs contactinformatie;
11. maatregelen om de veiligheid van de in het plan vervatte informatie te waarborgen;
12. maatregelen om een doeltreffende beveiliging van lading en laad- en losapparatuur binnen de havenfaciliteit te waarborgen;
13. procedures voor het controleren van het veiligheidsplan van de havenfaciliteit;
14. reactieprocedures wanneer het scheepsveiligheidsalarmsysteem in de havenfaciliteit is geactiveerd;
15. procedures ter vergemakkelijking van walverlof voor het scheepspersoneel of personeelswisselingen en van de toegang van bezoekers tot het schip, waaronder afgevaardigden van welzijns- en vakbondsorganisaties voor zeelieden.

Uit dit artikel en met name uit lid 3 sub 2 volgt dat er door een ISPS-bedrijf maatregelen worden genomen om te voorkomen dat onbevoegden toegang krijgen tot het terrein en/of andere aangemeerde schepen.

Bijlage II, deel A

Artikel 17 lid 2

De taken en verantwoordelijkheden van een veiligheidsbeambte van de havenfaciliteit omvatten, naast die welke elders in dit Deel van de Code vermeld staan, onder meer:

1. uitvoering van een eerste uitgebreid veiligheidsonderzoek van de havenfaciliteit, waarbij rekening wordt gehouden met de betreffende veiligheidsbeoordeling van de havenfaciliteit;
2. de zorg voor ontwikkeling en onderhoud van het havenfaciliteitsveiligheidsplan;
3. de uitvoering van het havenfaciliteitsveiligheidsplan en de daarmee verband houdende oefeningen;
4. de regelmatige uitvoering van veiligheidsinspecties in de havenfaciliteit om ervoor te zorgen dat passende veiligheidsmaatregelen gehandhaafd blijven;
5. aanbevelingen doen voor wijzigingen van het havenfaciliteitsveiligheidsplan en deze daarin aanbrengen, naar gelang van toepassing, teneinde onvolkomenheden te corrigeren en het plan bij te werken in verband met van belang zijnde veranderingen in de havenfaciliteit;
6. verhoging van de veiligheidsbewustheid en de waakzaamheid van het personeel van de havenfaciliteit;
7. zorgen dat het personeel dat verantwoordelijk is voor de beveiliging van de havenfaciliteit voldoende getraind is;
8. rapportage aan de betreffende autoriteiten en documentering van documentatie met betrekking tot voorvallen die bedreigend zijn voor de veiligheid van de havenfaciliteit;
9. coördinatie van de uitvoering van het havenfaciliteitsveiligheidsplan met de betreffende veiligheidsbeambten van de maatschappij en de schepen;
10. coördinatie met veiligheidsdiensten;
11. zorgen dat wordt voldaan aan de normen die gelden voor personeel dat verantwoordelijk is voor de beveiliging van de havenfaciliteit;
12. het waarborgen dat eventueel aanwezige veiligheidsapparatuur op de juiste wijze wordt gebruikt, getest, geijkt en onderhouden; en
13. scheepsveiligheidsbeambten, indien zij dit vragen, helpen bij de vaststelling van de identiteit van mensen die zich willen inschepen.

Uit dit artikel en met name uit sub 8 volgt dat de PFSO gehouden is om voorvallen die bedreigend zijn voor de veiligheid van een ISPS-bedrijf te melden aan de autoriteiten. Dit gebeurt in de praktijk door een melding aan het ISPS-meldpunt van de politie (meldformulier).

Bijlage III, deel B, artikel 4 leden 37 t/m 41

Artikel 4.37

Voorschrift XI-2/9.2.1 geeft een overzicht van de informatie die verdragsluitende staten van een schip mogen eisen als voorwaarde om een haven te mogen binnenkomen. Een van de punten in het overzicht is de bevestiging van enigerlei speciale of extra maatregelen die door het schip zijn genomen tijdens zijn laatste tien keer afmeren bij een havenfaciliteit. Hier volgen twee voorbeelden:

1. documentatie van de getroffen maatregelen tijdens het bezoek aan een havenfaciliteit die zich bevindt op het grondgebied van een staat die geen verdragsluitende staat is, met name van die maatregelen die normaal gesproken zouden zijn getroffen door havenfaciliteiten die zich bevinden op het grondgebied van verdragsluitende staten; en

2. eventuele Verklaringen van Veiligheid die zijn aangegaan met havenfaciliteiten of andere schepen.

Artikel 4.38

Een ander punt van informatie dat in het overzicht is opgenomen en dat kan worden verlangd als voorwaarde om de haven binnen te mogen, is de bevestiging dat er tijdens activiteiten tussen schepen onderling die werden uitgevoerd tijdens de periode van de laatste tien keer afmeren bij een havenfaciliteit, geschikte scheepsveiligheidsprocedures zijn gehanteerd. Het is doorgaans niet nodig de overdracht van loodsen of van douane-, immigratie of veiligheidsbeambten, noch het bunkeren, lichten, laden van voorraden en het lossen van afval door het schip binnen havenfaciliteiten te documenteren, omdat deze activiteiten normaal gesproken binnen de verantwoordelijkheid van het havenfaciliteitveiligheidsplan vallen. Hier volgen enkele voorbeelden van te verstrekken informatie:

1. documentatie van de getroffen maatregelen tijdens activiteiten tussen schepen onderling met een schip dat onder de vlag vaart van een staat die geen verdragsluitende staat is, met name van die maatregelen die normaal gesproken zouden zijn getroffen door schepen die onder de vlag van verdragsluitende staten varen;
2. documentatie van de getroffen maatregelen tijdens activiteiten tussen schepen onderling met een schip dat onder de vlag vaart van een verdragsluitende staat, maar dat niet hoeft te voldoen aan de bepalingen van hoofdstuk XI-2 en deel A van deze Code, zoals een exemplaar van een veiligheidscertificaat dat krachtens andere bepalingen aan dat schip is afgegeven; en
3. in het geval dat er personen of goederen aan boord zijn die uit zee zijn gered, alle bekende informatie over dergelijke personen of goederen, inclusief hun identiteit – indien deze bekend is — en de resultaten van eventuele namens het schip uitgevoerde controles ter vaststelling van de veiligheidsstatus van de geredde personen of goederen. Het is niet de intentie van hoofdstuk XI-2 of deel A van deze Code om de aflevering van mensen die op zee in moeilijkheden zijn aangetroffen in een veilige haven te vertragen of te verhinderen. Hoofdstuk XI-2 en deel A van deze Code hebben als enige intentie staten voldoende geschikte informatie te verschaffen om het behoud van hun integriteit op het gebied van veiligheid te waarborgen.

Artikel 4.39

Hier volgen enkele voorbeelden van andere praktische, met veiligheid verband houdende informatie die kan worden verlangd als voorwaarde om een haven binnen te mogen teneinde bij te dragen aan de waarborging van de veiligheid en beveiliging van personen, havenfaciliteiten, schepen en andere eigendommen:

1. informatie in het Continu Overzichtsrapport;
2. locatie van het schip op het tijdstip waarop het rapport wordt gemaakt;
3. verwachte aankomsttijd van het schip in de haven;
4. bemanningslijst;
5. algemene omschrijving van lading aan boord van het schip;
6. passagierslijst; en
7. informatie die moet worden meegevoerd krachtens voorschrift XI-2/5.

Artikel 4.40

Voorschrift XI-2/9.2.5 stelt de kapitein van een schip, zodra deze op de hoogte is gesteld van het voornemen van de kust- of havenstaat om beperkende maatregelen krachtens voorschrift XI-2/9.2 ten uitvoer te leggen, in staat van de intentie om het schip de haven te laten aandoen, af te zien. Als de kapitein van die intentie afziet, is voorschrift XI-2/9 niet langer van toepassing en enige andere stappen die worden genomen moeten gebaseerd zijn op en in overeenstemming met internationaal recht.

Artikel 4.41

In alle gevallen waarbij een schip de toegang tot een haven wordt ontzegd of uit een haven wordt verdreven, dienen alle bekende feiten ter kennis te worden gebracht van de autoriteiten van relevante staten. Deze kennisgeving dient te bestaan uit de volgende punten, indien bekend:

1. naam van het schip, de vlag waaronder het schip vaart, scheepsidentificatienummer, roepletters van het schip, scheepstype en lading;
2. reden van toegangsweigering of van uitzetting uit haven of havengebieden;
3. indien relevant, de aard van enigerlei afwijking van de veiligheidsvoorschriften;
4. indien relevant, nadere gegevens van pogingen die zijn ondernomen om afwijkingen van de veiligheidsvoorschriften te corrigeren, waaronder begrepen eventuele voorwaarden die voor de reis aan het schip zijn opgelegd;
5. vorige aanloophaven(s) en eerstvolgende bekende aanloophaven;
6. vertrektijd en geschatte waarschijnlijke aankomsttijd in die havens;
7. enige aan het schip verstrekte instructies, bijv. rapportage over de route;
8. beschikbare informatie over het veiligheidsniveau waarbij het schip op dat moment opereert;
9. informatie over enigerlei communicatie tussen de havenstaat en de overheid;
10. aanspreekpunt binnen de havenstaat dat het rapport opmaakt om nadere informatie te verkrijgen;
11. bemanningslijst; en
12. enige andere relevante informatie.

Uit deze artikelen en met name uit artikelen 4.39 en 4.41 volgt welke informatie, waaronder de bemanningslijst en andere persoonsgegevens, van een schip mag worden opgevraagd.

Bijlage III, deel B, artikel 16 lid 13

Artikel 16.13

Degenen die op verzoek niet willen of niet kunnen aantonen wat hun identiteit is en/of bevestigen wat het doel van hun bezoek is, dient toegang tot de havenfaciliteit te worden ontzegd, en hun poging toegang te verkrijgen dient te worden gerapporteerd aan de havenveiligheidsbeambte en aan de nationale of plaatselijke autoriteiten met beveiligingstaken.

Uit dit artikel volgt dat iemand de toegang moet worden ontzegd wanneer die zich niet kan of wil laten identificeren en dat de poging om toegang te krijgen en de weigering moet worden gerapporteerd aan de havenbeveiligingsbeambte en aan de nationale of plaatselijke autoriteiten met beveiligingstaken.

Bijlage III, deel B, artikel 16 leden 14 en 15

Artikel 16.14

In het HVP dienen de locaties te zijn geïdentificeerd waar het fouilleren van personen en het doorzoeken van persoonlijke bezittingen en voertuigen moeten plaatsvinden. Dergelijke locaties dienen overdekt te zijn, teneinde een ononderbroken functioneren, overeenkomstig de frequentie die in het HVP is vastgelegd, ongeacht lastige weersomstandigheden, te vergemakkelijken. Wanneer personen moeten worden gefouilleerd of persoonlijke bezittingen en voertuigen moeten worden doorzocht, dienen deze personen, persoonlijke bezittingen en voertuigen onmiddellijk naar afgesloten plaatsen voor aanhouding, inscheping of het laden van auto's te worden verplaatst.

Artikel 16.15

In het HVP dienen afzonderlijke locaties te zijn vastgesteld voor wel en niet gecontroleerde personen en hun bezittingen, en, indien mogelijk, afzonderlijke plaatsen voor het inschepen/ontschepen van passagiers, en de bemanningsleden en hun bezittingen teneinde te waarborgen dat niet gecontroleerde personen niet in contact kunnen komen met wel gecontroleerde personen.

Uit deze artikelen volgt dat een ISPS-bedrijf maatregelen moet nemen om identificatie en, indien nodig fouillering, ordentelijk te laten plaatsvinden o.a. door niet gecontroleerde te scheiden van wel gecontroleerde mensen.

Bijlage III, deel B, artikel 16 lid 17

Artikel 16.17

Voor veiligheidsniveau 1 dienen in het HVP de controlepunten te zijn vastgesteld waar de volgende veiligheidsmaatregelen kunnen worden toegepast:

1. gebieden waarvoor beperkingen gelden, die door middel van hekken of andere hindernissen omheind dienen te zijn volgens normen die door de verdragsluitende staat dienen te zijn goedgekeurd;
2. het controleren van de identiteit van alle personen die in verband met de aanwezigheid van een schip toegang tot de havenfaciliteit willen verkrijgen, waaronder passagiers, bemanningsleden en bezoekers, en het aantonen van hun redenen hiertoe door bijvoorbeeld instructies zich te vervoegen, passagierstickets, pasjes, werkorders, enz. te controleren;
3. het controleren van voertuigen die worden gebruikt door degenen die in verband met de aanwezigheid van een schip toegang tot de havenfaciliteit willen verkrijgen;
4. het verifiëren van de identiteit van personeel van de havenfaciliteit en degenen die binnen de havenfaciliteit werkzaam zijn en hun voertuigen;
5. het beperken van toegang om degenen die niet in dienst van de havenfaciliteit zijn of daarbinnen werkzaam zijn uit te sluiten, indien zij niet in staat zijn hun identiteit aan te tonen;
6. het fouilleren van personen en het doorzoeken van persoonlijke bezittingen, voertuigen en hun inhoud; en
7. het identificeren van alle toegangspunten waar geen regelmatig gebruik van wordt gemaakt, die permanent dicht en afgesloten dienen te zijn.

Uit dit artikel volgt dat een ISPS-bedrijf de identiteit moet controleren van iedereen die toegang wil. Indien nodig mag daarbij worden gefouilleerd en mogen de bezittingen worden doorzocht; mits dit is goedgekeurd door de Staat. Degenen die toegang willen, dienen aan te tonen wat de reden daartoe is. Ook voertuigen kunnen worden gecontroleerd.

Koppeling met de Gedragscode

Uit de bovenbeschreven regelgeving volgt dat het voor een ISPS-bedrijf noodzakelijk is om een beveiligings- en veiligheidsbeleid te voeren. Een noodzakelijk onderdeel daarvan is het toegangsbeleid. Bij een gedegen uitvoering van het toegangsbeleid worden persoonsgegevens verwerkt. Een ISPS-bedrijf verwerkt dus persoonsgegevens bij het uitvoeren van cq. voldoen aan de in deze bijlage beschreven regelgeving.

Bijlage 12 - Protocol overheidspersoneel

Protocol Toegang havenfaciliteiten voor overheidsambtenaren

A. Begripsbepaling

Overheidsambtenaren zijn in deze:

1. Toezichthouders als omschreven in artikel 5:11 van de Algemene Wet Bestuursrecht in de rechtmatige uitoefening van hun taak, en
2. Opsporingsambtenaren als bedoeld in artikelen 141 en 142 van het Wetboek van Strafvordering in de rechtmatige uitoefening van hun taak.
3. Ambtenaren als bedoeld in de Wet op de Inlichtingen- en Veiligheidsdiensten 2002.

Alle andere overheidsambtenaren vallen **niet** onder dit protocol.
De rechten voortvloeiend uit artikel 5:15 Awb en artikel 8 Politiewet kunnen niet beperkt worden door de beveiligingsplannen van havenfaciliteiten dan wel schepen. Dit betekent dat genoemde ambtenaren **niet verplicht** kunnen worden medewerking te verlenen aan vormen van toegangscontrole zoals deze bij de havenfaciliteiten geldend zijn. Bovendien kan hen niet de toegang ontzegd worden indien zij géén medewerking verlenen aan de toegangscontrole. Desalniettemin is het verstandig een zekere modus vivendi te zoeken om te voorkomen dat slechte verstandhoudingen gaan ontstaan tussen overheidsdiensten en bedrijven/terminals

B. Instructies

Om conflictsituaties te voorkomen dienen de overheidsambtenaren en beheerders van havenfaciliteiten de volgende instructies in acht te nemen:

1. Verifieer op welke security level de havenfaciliteit zich bevindt:
    a. Level 1: Vervolg werkzaamheden
    b. Level 2: Overweeg werkzaamheden uit te stellen tot level 1 situatie aan de orde is. Indien niet mogelijk, vervolg werkzaamheden.
    c. Level 3: De werkzaamheden vinden geen of beperkt doorgang; volg instructies op.
2. Zij dienen zichzelf en de dienst waarvoor zij werken mondeling bekend te maken;
3. Zij dienen altijd hun legitimatiebewijs te tonen. Hiervan mag géén kopie worden gemaakt(1);
4. Zij dienen herkenbaar te zijn als ambtenaren van een specifieke overheidsdienst(2);
5. Desgewenst tekenen ze een bezoekersregistratie en verstrekken een contactnummer bij de dienst waarvoor zij werken opdat bij gerede vermoeden van twijfel omtrent de identiteit verificatie kan plaatsvinden;
6. Visitatie van bagage, meegenomen apparatuur alsmede voertuig is niet toegestaan;
7. Veiligheidsfouillering van de ambtenaren is niet toegestaan, tenzij dit gevorderd wordt door een opsporingsambtenaar (bijv. bij een verhoogd security level);
8. zij staan toe dat ze eventueel vergezeld worden door een medewerker van de beveiligingsdienst van de havenfaciliteit. Dit mag echter geen belemmering zijn bij de uitvoering van de werkzaamheden.

(1) Ivm bescherming privacy -> personen treden op namens de overheid, niet als privé-persoon
(2) Middels specifieke kleding, voertuigen, etc..

NB

1. De bovenstaande instructies brengen met zich mee dat de betreffende overheidsdienst zelf garant staat voor de betrouwbaarheid van haar medewerkers. Deze diensten moeten dan ook zelf onderzoeken in hoeverre zij maatregelen moet treffen en zo ja, welke. Tegelijkertijd brengt het benoemen van opsporingsambtenaren resp. toezichthouders al met zich mee dat reeds handelingen verricht zijn t.a.v. de betrouwbaarheid van de medewerkers.
2. Alle havenfaciliteiten zouden de beschikking moeten hebben over specimen van de diverse identiteitsbewijzen van overheidsdiensten.

PORT PRIVACY

Bijlage 13 - Vitale sector

De Rotterdamse haven is door de overheid aangemerkt als een vitale sector: een sector met vitale processen op het gebied van scheepvaartafwikkeling en transport (zie bijvoorbeeld de bijgevoegde factsheet van de Rijksoverheid en voorts het Besluit meldplicht cybersecurity uit december 2017).

Een vitale sector is een sector die cruciaal is voor het goed functioneren van de Nederlandse maatschappij en als een sector die tot ontwrichting van de samenleving zou leiden wanneer de processen in die sector zouden uitvallen. Van ontwrichting is sprake wanneer er veel slachtoffers vallen, wanneer er sprake is van grote economische schade of wanneer herstel heel lang gaat duren en er geen reële alternatieven zijn terwijl de samenleving deze producten en diensten niet kan missen.

ISPS-bedrijven vormen het kloppende hart van de Rotterdamse haven. Zij hebben de belangrijke taak en zware verantwoordelijkheid om zorg te dragen voor de veiligheid, de beveiliging en de continuïteit van de vitale bedrijfsprocessen met als doel de samenleving tegen ontwrichting te beschermen.

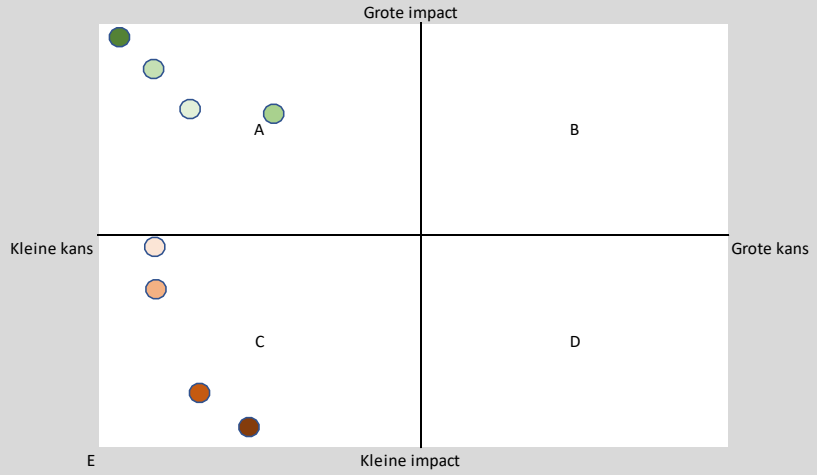
Het belang van veiligheid ziet op het voorkomen van ongelukken, incidenten, rampen, enz. die een bedreiging vormen voor de gezondheid van personeel en de volksgezondheid van de mensen in de nabije en verre omgeving van het havengebied. Het belang van beveiliging ziet op het voorkomen van criminaliteit en terreurdaden, enz. Het bewaken van de continuïteit is in het belang van het ISPS-bedrijf zelf èn van de duizenden bedrijven en daarmee gezinnen die afhankelijk zijn van een soepel lopende haveneconomie.

Rotterdam is al jaren lang de grootste haven van Europa en één van de grootste havens van de wereld. Het economisch belang van de wereldhaven is enorm. Dag in, dag uit worden uit alle landen van de aarde goederen aangeleverd. Van appels tot auto’s, van computers tot ijzererts. In het Rotterdamse havengebied worden ieder jaar meer dan 100.000 schepen en binnenvaartschepen gelost en geladen. Iedere dag vertrekken er talloze vrachtwagens met lading naar alle uithoeken van Europa. Ook worden goederen verwerkt tot industriële producten. Raffinaderijen maken van de aangevoerde ruwe olie grondstoffen voor de chemische industrie. De chemische bedrijven maken vervolgens grote hoeveelheden halffabricaten, waarvan elders in de wereld eindproducten worden gemaakt in de vorm van verf of plastic materiaal. Steenkool en ijzererts worden aangevoerd voor elektriciteitscentrales en de auto-industrie in het Duitse Ruhrgebied. Via de Rijn en andere verbindingswegen vinden al deze goederen hun weg naar honderden miljoenen Europeanen. Circa 175.000 banen zijn direct of indirect afhankelijk van de haveneconomie waarvan de ISPS-bedrijven de motor vormen. De directe toegevoegde waarde van de Rotterdamse haven bedroeg in 2015 ruim 12 miljard euro. De directe en indirecte toegevoegde waarde bedroeg bijna 21 miljard euro. Dat is 3,1 % van het Nederlandse bruto binnenlandse product (feiten & cijfers Havenbedrijf Rotterdam).

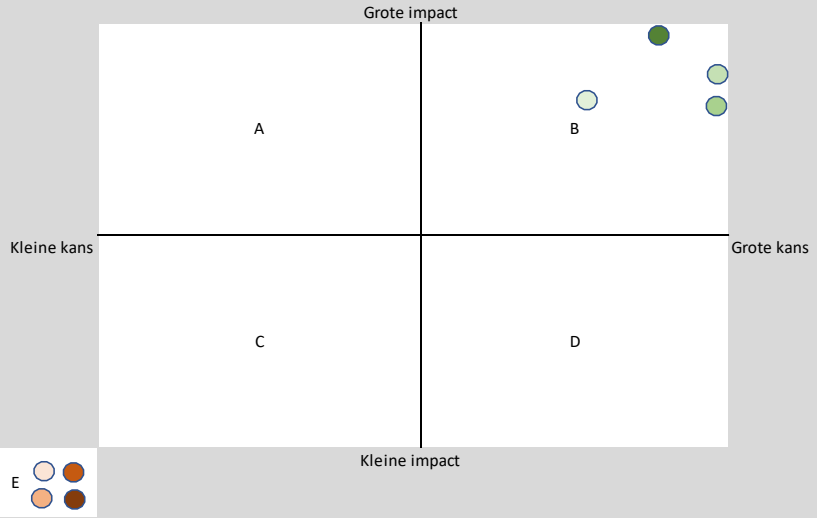
In het kader van de genoemde vitale belangen heeft elk ISPS-bedrijf een veiligheidsbeleid. Cruciaal onderdeel van een passend, efficiënt en effectief veiligheid- en beveiligingsbeleid is een betrouwbaar en sluitend toegangscontrolebeleid. Het voeren van een gedegen toegangscontrolebeleid sluit niet voor niets naadloos aan bij de eisen die de ISPS-regelgeving stelt (regelgeving die is ontstaan na de aanslagen van 9/11). Het is noodzakelijk om als ISPS-bedrijf te weten wie er wanneer en om welke reden op het terrein aanwezig is of was. Om daadwerkelijk te kunnen nagaan of iemand degene is voor wie hij zich uitgeeft, is het in voorkomende gevallen noodzakelijk om bijzondere persoonsgegevens te verwerken, zoals een pasfoto (bijvoorbeeld om te voorkomen dat iemand met een gestolen toegangskaart toch toegang heeft tot een ISPS-bedrijf). Zonder dit beleid lopen de vitale processen vast en dreigt een ontwrichting van de samenleving.

Bijlage 14 - Belangenafweging gerechtvaardigd belang

RISICO-INSCHATTING - Met toegangsbeleid



RISICO-INSCHATTING - Zonder toegangsbeleid



		Met toegangsbeleid	Zonder toegangsbeleid
1	Identiteitsdiefstal	C	E
2	Reputatieschade	C	E
3	Stress	C	E
4	Beperking in bewegingsvrijheid	C	E
5	Veiligheidsincident giftige stoffen	A	B
6	Maatschappelijke ontwrichting als gevolg van stagnatie	A	B
7	Drugscriminaliteit	A	B
8	Terroristische aanslag	A	B

Bijlage 15 - Biometrische verificatie

Juridisch kader
Biometrische persoonsgegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

Het verwerken van biometrische persoonsgegevens met het oog op de unieke identificatie van een persoon is verboden. Op dit verbod is een uitzondering gemaakt in artikel 29 UAVG. Het verbod is niet van toepassing indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Authenticatie en beveiliging
Van die laatste uitzondering is sprake bij het verwerken van biometrische gegevens in het kader van het toegangsbeleid van ISPS-bedrijven.

Biometrische verificatie in het kader van het toegangsbeleid van ISPS-bedrijven wordt ingezet om te kunnen vaststellen dat degene is wie hij stelt te zijn (authenticatie) en om te voorkomen dat toegang wordt verleend aan onbevoegden (beveiliging).

Het gebruik van biometrische toegangskaarten brengt het beveiligingsniveau naar een passend en noodzakelijk hoog niveau. Het zorgt er voor dat een ISPS-bedrijf er (nagenoeg volledig) zeker van kan zijn dat degene die de toegangskaart aanbiedt, bevoegd is om zich toegang tot het terrein te verschaffen. Diefstal of het uitlenen van een toegangskaart heeft immers geen zin meer. Daarmee wordt onbevoegde toegang en identiteitsfraude voorkomen, criminaliteit teruggedrongen en de veiligheid van zowel het ISPS-bedrijf als de betrokkene gediend.

Bovendien zorgt het gebruik van biometrische toegangskaarten er voor dat het bedrijfsproces veel efficiënter verloopt. Het proces aan de poort waarbij een betrokkene zich moet identificeren geschiedt vele malen sneller en trefzekerder. Het voorkomt lange files aan de toegangspoorten en stagnatie van de motor van de Nederlandse economie.

Tot slot zijn er minder beveiligers bij het proces betrokken en hoeft een betrokkene zich minder vaak te legitimeren door het tonen van een identiteitsbewijs hetgeen minder belastend is voor zowel het ISPS-bedrijf als (de privacy van) de betrokkene.

Uitgifte en activering
De toegangskaart wordt verstrekt door een extern bedrijf dat voldoet aan de ISO-norm 27001 voor informatiebeveiliging en dat daartoe contracten heeft gesloten met het ISPS-bedrijf en het bedrijf of de organisatie waar de betrokkene werkzaam voor is.

De betrokkene (of diens werkgever of een intermediaire partij) ontvangt van het externe bedrijf/organisatie in separate brieven een inactieve toegangskaart, een activeerbrief en een pincode. Met de activeerbrief en de pincode kan de toegangskaart door de betrokkene worden geactiveerd op een activeringspunt.

Tijdens de activeringsprocedure wordt het aderpatroon van één of meer van de vingers (‘finger vein’) of de hele hand van de betrokkene gescand en gebruikt als rekenmiddel om een binaire code (een binaire template) te genereren. Deze binaire code wordt direct versleuteld (encryptie) en is niet meer terug te leiden naar de betrokkene (non reverse enginerable). De binaire code wordt opgeslagen op de toegangskaart van de betrokkene.

Gebruik
Bij het gebruik van de toegangskaart wordt zowel de toegangskaart als één van de vingers of hele hand aangeboden aan een uitleesapparaat aan de toegangspoort van het ISPS-bedrijf. Met de scan van de vinger(s) of de hand wordt direct een berekening gemaakt zoals hierboven is beschreven. Wanneer de uitkomst gelijk is aan de binaire code op de toegangskaart wordt toegang verleend. Met deze tweestapsverificatie wordt voorkomen dat iemand met een gestolen toegangskaart toegang wordt verleend.

Bijlage 16 - Protocollen privacyrechten

Protocol voor het recht op inzage
Inleiding

Wanneer iemand aanspraak maakt op zijn recht op inzage worden de volgende stappen doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs. Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Welke persoonsgegevens worden verwerkt?
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt.

Stap 5 – Informatieoverzicht
Stel een overzicht op met de navolgende elementen en geef de verzoeker inzage door het overzicht toe te sturen:

Persoonsgegevens (of categorieën van)	Om welke persoonsgegevens gaat het? (zie vorige stap)
Verwerkingsdoeleinden	Wat is het doel van de verwerking van persoonsgegevens?
Ontvangers (of categorieën van)	Worden de persoonsgegevens doorgestuurd? Aan wie?
Bewaartermijn (of criteria daarvoor)	Hoe lang worden de persoonsgegevens bewaard?
Privacyrechten	Wijs de verzoeker op diens recht op rectificatie, wissing, beperking en bezwaar en op het recht om een klacht in te dienen bij de AP
Bron	Informeer over de bron van de persoonsgegevens in het geval

	deze niet van de betrokkene zelf zijn ontvangen
Automatische besluitvorming	Informeer de verzoeker over het bestaan van geautomatiseerde besluitvorming en profiling en over de achterliggende logica in het geval dat aan de orde is
Doorgifte aan 3e landen	Informeer de betrokkene over de genomen waarborgen in het geval persoonsgegevens worden verstrekt aan landen of organisaties buiten de EU

Geachte [heer/mevrouw] [naam],

In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij persoonsgegevens van u verwerken. Ik voorzie u daarom van het navolgende overzicht.

Categorie persoonsgegevens	*Doelen*	*Ontvangers*	*Bewaartermijnen*	*Bron*	*Informatie over de bron*

Voor de goede orde merken wij op dat er geen sprake is van automatische besluitvorming op basis van de door ons ontvangen/verzamelde persoonsgegevens. Voorts vindt er geen doorgifte plaats naar landen of organisaties buiten de EU.

Tot slot wijzen wij u op uw recht op rectificatie, wissing en beperking. Voorts heeft het recht om bezwaar te maken en om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Wij gaan er evenwel vanuit dat in het geval u vragen of opmerkingen heeft, u deze eerst aan ons voorlegt.

Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.

Met vriendelijke groet,
[bedrijfsnaam]
[naam], privacy officer

Stap 6 – Dossiervorming

Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op kopie

Inleiding
Wanneer iemand aanspraak maakt op zijn recht op een kopie moeten de navolgende stappen worden doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Voor de goede orde wordt opgemerkt dat wanneer wordt besloten om uw verzoek te honoreren er voor het verstrekken van een kopie geen kosten in rekening worden gebracht maar dat wanneer u om bijkomende kopieën verzoekt, een redelijke vergoeding zal worden verlangd.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs. Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Kopie
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt, maak daar een kopie van en stuur de kopie toe aan de verzoeker.

Let op dat hierbij geen inbreuk wordt gemaakt op de privacyrechten van anderen.

Stap 5 – Dossiervorming
Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op rectificatie of aanvulling

Inleiding
Wanneer iemand aanspraak maakt op zijn recht op rectificatie of aanvulling moeten de navolgende stappen worden doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude e/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs. Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Welke persoonsgegevens worden verwerkt?
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt.

Stap 5 – Controleer de juistheid, rectificeer of vul aan indien nodig en informeer verzoeker
Ga na of de door de verzoeker verzochte wijziging juist is. Is dit het geval wijzig de persoonsgegevens dan dienovereenkomstig en informeer de verzoeker hierover.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Hierbij berichten wij u dat wij de door u verzochte rectificatie en/of aanvulling hebben doorgevoerd.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 6 – Dossiervorming
Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op dataportabiliteit

Inleiding
Wanneer iemand aanspraak maakt op zijn recht op dataportabiliteit (overdraagbaarheid) moeten de navolgende stappen worden doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs.

Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Beoordeel het verzoek
Ga na of het verzoek dient te worden gehonoreerd. Een betrokkene heeft het recht op overdracht van zijn persoonsgegevens indien:

- de gegevens door de betrokkene zijn verstrekt en
- de verwerking plaatsvindt op grond van (uitdrukkelijke) toestemming of op grond van een overeenkomst waarbij de betrokkene partij is en de verwerkingen plaatsvinden via geautomatiseerde procedés.

Stap 5 – Besluit op het verzoek en informeer de betrokkene en (eventueel) draag over
Neem naar aanleiding van de beoordeling een besluit, informeer de betrokkene hierover en (wanneer tot overdracht wordt besloten:) draag de persoonsgegevens over in een gestructureerde, gangbare en machineleesbare vorm aan de betrokkene of (indien de betrokkene dit wenst) aan een andere verwerkingsverantwoordelijke.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] bericht ik u dat wij aan uw verzoek zullen voldoen.*
>
> *[uitleg over hoe, wanneer en aan wie de gegevens worden overgedragen].*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*

[naam], privacy officer

Stap 6 – Dossiervorming

Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op wissing (vergetelheid)

Inleiding
Wanneer iemand aanspraak maakt op zijn recht op wissing (vergetelheid) moeten de navolgende stappen worden doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs.

Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Welke persoonsgegevens worden verwerkt?
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt.

Stap 5 – Ga na of het verzoek gerechtvaardigd is
Ga na of aan het verzoek moet worden voldaan. Aan een verzoek om wissing van persoonsgegevens moet worden voldaan indien:

- de persoonsgegevens niet langer nodig zijn voor het doel
- er voor de verwerking geen grondslag (meer) is (bijvoorbeeld wanneer de verwerking was gebaseerd op de toestemming van de betrokkene maar die de toestemming is ingetrokken)
- betrokkene bezwaar maakt en diens belangen zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke
- er sprake is van onrechtmatige verwerking
- dit volgt uit de wet.

Stap 6 – Informeer de betrokkene
Besluit of het verzoek gehonoreerd moet worden en informeer de betrokkene.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Hierbij berichten wij u dat wij aan uw verzoek hebben voldaan en wij per [datum] geen persoonsgegevens meer van u verwerken.*

[Omdat uw persoonsgegevens door ons ook openbaar zijn gemaakt, hebben wij alle redelijkerwijs van ons te vergen maatregelen genomen om andere verwerkingsverantwoordelijken te informeren over uw verzoek om iedere koppeling naar, of kopie of reproductie van uw persoonsgegevens te wissen.]

Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.

Met vriendelijke groet,
[bedrijfsnaam]
[naam], privacy officer

Stap 7 – Dossiervorming

Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op beperking van verwerking

Inleiding
Wanneer iemand aanspraak maakt op zijn recht op beperking van verwerking (en dus verzoekt om een deel van de persoonsgegevens (tijdelijk) niet meer te verwerken), worden de volgende stappen doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen verzoek
Meld aan de verzoeker dat het verzoek alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs.

Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval (of gaat het om een onredelijk of excessief verzoek) laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Welke persoonsgegevens worden verwerkt?
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt.

Stap 5 – Beoordeling van het verzoek
Beoordeel het verzoek om een deel van de persoonsgegevens (tijdelijk) niet meer te verwerken.

Een beperking is verplicht indien:
- de juistheid wordt betwist (gedurende de periode waarin dit wordt onderzocht)
- de verwerking onrechtmatig is
- de betrokkene de persoonsgegevens nog nodig heeft ten behoeve van een rechtsvordering terwijl de verwerkingsverantwoordelijke de gegevens niet langer voor zijn doel nodig heeft
- de betrokkene bezwaar maakt (gedurende de periode dat wordt onderzocht of diens belangen zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke).

Stap 6 – Neem een besluit en informeer de verzoeker
Neem een besluit en informeer de verzoeker.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij persoonsgegevens van u verwerken. U heeft verzocht om [een deel van] de persoonsgegevens [tijdelijk] niet meer te verwerken.*

Hierbij berichten wij dat wij aan uw verzoek tegemoet komen. Dit betekent dat wij [uitleg over welke (categorie van) persoonsgegevens niet meer worden verwerkt; en eventueel voor welke periode dit zal gelden].

In het geval wij te zijner tijd de persoonsgegevens toch weer gaan verwerken, ontvangt u daarvan eerst bericht van ons.

Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.

Met vriendelijke groet,
[bedrijfsnaam]
[naam], privacy officer

Stap 7 – Dossiervorming
Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol voor het recht op bezwaar

Inleiding
Wanneer iemand bezwaar maakt tegen de verwerking van persoonsgegevens moeten de navolgende stappen worden doorlopen.

Bij sommige stappen is een voorbeeldtekst toegevoegd. Uiteraard dient de tekst te worden aangepast aan de omstandigheden van het geval.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 0 – Indienen bezwaar
Meld aan de verzoeker dat het bezwaar alleen kan worden ingediend per mail aan het adres [mailadres]; zoals dat ook staat vermeld in privacyverklaringen, en dat hij zich vervolgens zal moeten legitimeren.

Stap 1 – Ontvangstbevestiging
Bevestig per mail aan de verzoeker dat zijn verzoek ontvangen is. Meld daarbij dat hij zich eerst moet legitimeren en dat op zijn verzoek vervolgens uiterlijk binnen één maand zal worden gereageerd.

> *Geachte [heer/mevrouw] [naam],*
>
> *Hierbij bevestig ik de ontvangst van uw verzoek.*
>
> *Uit veiligheidsoverwegingen en om datalekken, fraude en/of misbruik van recht te voorkomen, zijn wij genoodzaakt om u eerst te identificeren. Wij verzoeken u daarom om naar ons kantoor te komen en om u daar te legitimeren met een geldig legitimatiebewijs. Het adres van ons kantoor staat onder aan dit bericht.*
>
> *Bij de identificatie wordt uw naam, het soort identiteitsbewijs en het kaartnummer genoteerd. Vervolgens word uw verzoek in behandeling genomen. Onze reactie op uw verzoek volgt dan zo spoedig mogelijk en uiterlijk binnen 1 maand. Wanneer blijkt dat er sprake is van complexiteit wordt deze termijn met 2 maanden verlengd. In dat geval ontvangt u daar binnen 1 maand bericht van.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 2 – Identificatie
Identificeer de verzoeker. Identificatie geschiedt door controle van een geldig identiteitsbewijs. Noteer de naam, het soort identiteitsbewijs en het kaartnummer van het identiteitsbewijs.

Noteer ook de datum waarop de identificatie plaatsvindt; dit is de startdatum van de termijn om op het verzoek te reageren.

Stap 3 – Worden er persoonsgegevens verwerkt?
Onderzoek of van verzoeker persoonsgegevens worden verwerkt en de verzoeker dus een betrokkene is in de zin van de AVG. Is dit niet het geval laat dit dan direct aan de verzoeker weten.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw verzoek d.d. [datum] hebben wij onderzoek gedaan. Uit het onderzoek is gebleken dat wij geen persoonsgegevens van u verwerken.*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 4 – Welke persoonsgegevens worden verwerkt?
Stel vast welke persoonsgegevens van de verzoeker worden verwerkt.

Stap 5 – Maak een nieuwe belangenafweging
Om te beslissen of aan het bezwaar tegemoet moet worden gekomen, moet een (nieuwe) afweging worden gemaakt tussen enerzijds het belang om de persoonsgegevens te verwerken en anderzijds het privacybelang van de betrokkene.

Stap 6 – Informeer de betrokkene
Besluit of aan het bezwaar tegemoet moet worden gekomen en informeer de betrokkene.

> *Geachte [heer/mevrouw] [naam],*
>
> *In reactie op uw bezwaar d.d. [datum] hebben wij onderzoek gedaan en opnieuw een afweging gemaakt tussen ons belang om uw persoonsgegevens te verwerken en uw privacybelang.*
>
> *Hierbij berichten wij u dat wij niet aan uw bezwaar tegemoet komen omdat [motivering].*
>
> *Wij vertrouwen er op u hiermee naar behoren en afdoende te hebben geïnformeerd. Heeft u nog vragen of opmerkingen dan vernemen wij uiteraard graag van u.*
>
> *Met vriendelijke groet,*
> *[bedrijfsnaam]*
> *[naam], privacy officer*

Stap 7 – Dossiervorming

Registreer het verzoek en de verwerking in (een apart onderdeel van) het verwerkingsregister.

Protocol meldplicht datalekken

Stap 1 – Stel vast of er sprake is van een datalek
Stel vast of er sprake is van een datalek.

Een datalek is een inbreuk op de beveiliging van persoonsgegevens waardoor: de persoonsgegevens per ongeluk of op onrechtmatige wijze worden vernietigd, verloren gaan of worden gewijzigd of de persoonsgegeven ongeoorloofd worden doorgestuurd of er ongeoorloofde toegang tot de persoonsgegevens plaatsvindt.

Voorbeelden van oorzaken van datalekken: kwijtgeraakte USB-stick, gestolen laptop, mail aan verkeerde personen, hack of inbraak in een datasysteem.

NB: Raadpleeg altijd een privacy expert om het protocol aan te passen aan en te implementeren in de organisatie.

Stap 2 – Meld het datalek aan de privacy officer
Meld een datalek altijd aan de privacy officer. Ook als er twijfel is over de vraag of het een datalek is, dient contact te worden opgenomen met de privacy officer.

Stap 3 – Stel de rol vast

Stel vast of het bedrijf ten aanzien van de persoonsgegevens die bij het datalek betrokken zijn, optreedt als verwerker of als verwerkingsverantwoordelijke.

Is er sprake van verwerkerschap, ga dan naar stap 4.
Is er sprake van verwerkingsverantwoordelijkheid, ga dan naar stap 5.

Stap 4 – Meld als verwerker het datalek aan de verwerkingsverantwoordelijke
Meld als verwerker een datalek direct, zonder onredelijke vertraging, aan de verwerkingsverantwoordelijke. Meld het datalek niet aan de Autoriteit persoonsgegevens: dat is een verplichting van de verwerkingsverantwoordelijke. Wees vervolgens behulpzaam in het traject waarin de verwerkingsverantwoordelijke omgaat met het datalek.

Stap 5 – Stel het privacy-risico vast
Stel vast of het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Stap 6 – Neem maatregelen
Neem maatregelen om het datalek aan te pakken met doel het datalek ongedaan te maken en/of om de schade te beperken en om datalekken in de toekomst te voorkomen.

Stap 7 – Meld het datalek bij de Autoriteit Persoonsgegevens (AP)
Is er waarschijnlijk sprake van een privacy risico meld het datalek dan bij de AP. Dit kan via het digitale loket op de website van de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0)

De melding moet worden gedaan binnen 72 uur nadat kennis is genomen van het datalek. Wordt die termijn niet gehaald dan moet dat worden gemotiveerd. Een melding kan eventueel in meerdere stappen worden gedaan.

In de melding moet ten minste worden opgenomen:
- de aard van het datalek
- indien mogelijk: de categorieën van en het aantal betrokkenen
- indien mogelijk: de categorieën van en het aantal persoonsgegevensregisters
- de naam en de contactgegevens van de privacy officer
- de waarschijnlijke gevolgen van het datalek
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of heeft genomen om het datalek aan te pakken (waaronder eventuele maatregelen om de schade te beperken).

Stap 8 – Meld het datalek aan de betrokkenen
Stel vast of het gaat om een hoog risico voor de rechten en vrijheden van natuurlijke personen. Is dat het geval meld het datalek dan ook, onverwijld, aan de betrokkenen, tenzij er sprake is van een uitzondering.

In de melding moet ten minste worden opgenomen:
- omschrijving van de aard van het datalek (in duidelijke en eenvoudige taal)
- de naam en de contactgegevens van de privacy officer
- de waarschijnlijke gevolgen van het datalek
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of heeft genomen om het datalek aan te pakken (waaronder eventuele maatregelen om de schade te beperken).

Uitzonderingen: een melding aan betrokkenen is niet verplicht als:
- er passende technische en organisatorische beschermingsmaatregelen zijn genomen (zoals met name versleuteling) ten aanzien van de persoonsgegevens die betrokken zijn bij het datalek;
- er achteraf maatregelen zijn genomen waardoor het bedoelde hoge risico zich waarschijnlijk niet meer zal voordoen
- de mededeling onevenredige inspanningen zou vergen (in plaats daarvan moet er dan een openbare mededeling plaatsvinden of een soortgelijke maatregel worden genomen).

Stap 9 – Dossiervorming
Registreer het datalek, de daarmee samenhangende feiten, de gevolgen en de genomen maatregelen in (een apart onderdeel van) het verwerkingsregister.

Bijlage 17 - Verzoek tot accreditatie

Verzoekschrift
Hierbij verzoekt Port Privacy B.V. (Port Privacy) de Nederlandse Autoriteit Persoonsgegevens om EBN Certification B.V. te accrediteren om te kunnen fungeren als extern toezichthoudend orgaan ten behoeve van de Privacy Gedragscode voor het toegangsbeleid van ISPS-bedrijven in Nederland.

Het verzoek is gebaseerd op artikel 41 lid 2 AVG en wordt ingediend in het kader van het verzoek tot goedkeuring van genoemde Gedragscode zoals bedoeld in artikel 40 lid 5 AVG. Beide verzoeken zijn tegelijkertijd bij de Autoriteit Persoonsgegevens ingediend.

Datum verzoek
Dit verzoek is ingediend op 17 september 2019.

Verzoeker
Het verzoek wordt gedaan door Port Privacy.

Contactpersoon	Tjeerd Poot
Adres	Nieuwe Sluisstraat 4a, 3111 PJ Schiedam
Website	www.portprivacy.com
Telefoonnummer	0624751388
Emailadres	tjeerdpoot@portprivacy.com

Werkgroep
De Gedragscode is opgesteld door Port Privacy in samenwerking met de Werkgroep. De Werkgroep bestaat uit een aantal ISPS-bedrijven en een aantal andere belanghebbenden.

Verwerkingsverantwoordelijke ISPS-bedrijven die lid zijn van de Werkgroep:
- APM Maasvlakte II B.V.
- APM Terminal Rotterdam B.V.
- European Bulk Services B.V.
- Europees Massagoed Overslagbedrijf B.V.
- Gate Terminal B.V.
- Huntsman Holland B.V.
- Hutchison Ports ECT Rotterdam B.V.
- Kramer Group B.V.
- Rotterdam World Gateway B.V.

Andere belanghebbenden die lid zijn van de Werkgroep:
- Belastingdienst Douane
- by DnA
- Havenbedrijf Rotterdam N.V.
- Royal Dirkzwager B.V.
- Secure Logistics B.V.

- Securitas Rotterdam B.V.
- Vereniging Deltalinqs
- Zeehavenpolitie

Vertegenwoordiging
Port Privacy vertegenwoordigt de Werkgroep. Dit blijkt uit de brieven in bijlage V1. De daarin ondertekende verklaringen luiden telkens:

> *Hierbij verklaar ik dat [bedrijfsnaam] lid is van de in deze brief bedoelde Werkgroep, de Werkgroep representatief is voor de sector van ISPS-bedrijven, Port Privacy de Werkgroep vertegenwoordigt in het project om te komen tot een of meer privacy gedragscodes voor het toegangsbeleid van Nederlandse ISPS-bedrijven en Port Privacy de Werkgroep dus vertegenwoordigt in haar communicatie en procedures met de Autoriteit Persoonsgegevens, o.a. in de goedkeuringsprocedure ex artikel 40 AVG.*

Bevoegde Toezichthoudende Autoriteit
Het verzoek is gericht aan de Nederlandse Autoriteit Persoonsgegevens (AP).

De AP is bevoegd om tot accreditatie van een toezichthoudend orgaan van een Gedragscode over te gaan omdat de verwerkingsactiviteiten waar de Gedragscode op ziet, plaatsvinden in Nederland en ook de verwerkingsverantwoordelijken, de verwerkers en de betrokkenen zich in Nederland bevinden, evenals de hoofdvestiging van Port Privacy en het toezichthoudend orgaan.

Toezichthoudend orgaan
Het verzoek betreft EBN Certification B.V. (EBN Certification).

EBN Certification is een externe, onafhankelijke certificerende instelling (CI) die een stabiele positie heeft ingenomen in de markt van certificerende instellingen. EBN Certification onderscheidt zich van de andere CI's door onder andere een goede toegankelijkheid, hoge mate van klantvriendelijkheid, doel- en oplossingsgericht, constructief kritisch alsmede respectvol naar individuen en de onderhavige managementsystemen.

EBN Certification voert onafhankelijke tweede en derde partij audits uit op eenmalige aanvraag en/of op langlopende overeenkomsten. Enerzijds onder auspiciën van de Raad van Accreditatie (RvA) daar waar het de eisen van geaccrediteerde schema's betreffen, en anderzijds audits op schema's die beheert en beheerst worden door brancheverenigingen of andere organisaties van belanghebbenden die niet onder eisen van de RvA vallen en derhalve niet geaccrediteerd zijn.

EBN Certification is lid van de Nederlandse Vereniging voor Certificatie-Instellingen (NVCI).

Contactpersoon	De heer C. van Zwienen
Adres	Heliotroopring 1100, 3316 KG Dordrecht
Website	www.ebncertification.nl
Telefoonnummer	0782003400
Emailadres	info@ebncertification.nl

Onderbouwing van het verzoek

Algemeen
EBN Certification voldoet aan de eisen van artikel 41 lid 2 AVG en de eisen van Hoofdstuk 12 van de Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

Dit betekent conform artikel 41 lid 2 AVG dat:

- EBN Certification onafhankelijk is;
- EBN Certification deskundig is met betrekking tot het onderwerp van de gedragscode;
- procedures zijn vastgesteld op grond waarvan EBN Certification kan beoordelen of de betrokken verwerkingsverantwoordelijken en verwerkers in aanmerking komen om de gedragscode toe te passen;
- procedures zijn vastgesteld op grond waarvan EBN Certification toezicht kan houden op de naleving van de bepalingen van de gedragscode;
- procedures heeft vastgesteld op grond waarvan EBN Certification de werking van de gedragscode op gezette tijden kan toetsen;
- procedures en structuren zijn vastgesteld om klachten te behandelen over inbreuken op de gedragscode of over de wijze waarop daaraan uitvoering is of wordt gegeven door een verwerkingsverantwoordelijke of verwerker;
- die procedures en structuren voor betrokkenen en het publiek transparant zijn gemaakt, en
- de taken en bevoegdheden van EBN Certification niet tot een belangenconflict leiden.

Ter onderbouwing van het bovenstaande geldt het volgende.

Onafhankelijkheid (12.1 Guidelines)
EBN Certification is een zelfstandige organisatie met de juiste mate van onafhankelijkheid, namelijk 100%. Zij heeft geen banden met de belanghebbenden van de Gedragscode, heeft niet deelgenomen aan de ontwikkeling van de Gedragscode en is volstrekt onpartijdig.

Haar onafhankelijkheid blijkt uit het navolgende:

- EBN Certification is door de RvA geaccrediteerd voor richtlijn ISO/IEC 17021-1:2015.
- EBN Certification heeft een Comité van Onafhankelijkheid ingesteld.
- EBN Certification hanteert voor haar personeel een gedragscode, een geheimhoudingsverklaring en een onafhankelijkheidsverklaring.

- Het certificatieproces van EBN Certification is volledig verifieerbaar en wordt periodiek gecontroleerd door de RvA.
- EBN Certification beschikt over een periodiek geactualiseerde risico-inventarisatie (RIE) waarmee haar onafhankelijkheid periodiek wordt gecontroleerd.
- EBN Certification heeft geen financiële banden met derden en is financieel onafhankelijk.

Accreditatie voor richtlijn ISO/IEC 17021-1:2015
EBN Certification is door de RvA geaccrediteerd voor richtlijn ISO/IEC 17021-1:2015. Dit blijkt uit de bijgaande accreditatieverklaring van de RvA (bijlage V2, bewijs van accreditatie door RvA). Dit betekent onder andere dat de RvA jaarlijks beoordeelt of EBN Certification onafhankelijk is en of procedures en structuren transparant zijn voor de betrokkenen en het publiek.

Comité van Onafhankelijkheid (CvO)
EBN Certification heeft een Committee for safegarding impartiallity, ofwel een Comité voor Onafhankelijkheid (CvO), ingesteld. De CvO heeft tot taak te toetsen of EBN Certification een onafhankelijke positie heeft en of haar dagelijkse werkwijze onafhankelijk is. De CvO bestaat uit een afspiegeling van belanghebbenden van de door EBN Certification gecertificeerde bedrijven/activiteiten en verricht haar taak door periodiek de processen binnen EBN Certification te beoordelen. Tijdens de jaarlijkse bijeenkomst wordt een vaste agenda gevolgd en wordt onder andere besproken: het gevolgde beleid, de financiële positie en het onafhankelijk functioneren van auditors en de risico-inventarisatie (bijlage V3, agenda CvO).

Gedragscode, geheimhoudingsverklaring en onafhankelijkheidsverklaring
EBN Certification hanteert een gedragscode die regels stelt aan haar werknemers en aan ingeschakelde externe arbeidskrachten met betrekking tot integriteit, vertrouwelijkheid en respect (bijlage V4, gedragscode). Voorts is het personeel gehouden geheimhouding te verklaren (bijlage V5, geheimhoudingsverklaring). Bovendien zijn auditoren van EBN Certification gehouden om per audit (nogmaals) te verklaren onafhankelijk te zijn (bijlage V6, werkorder met onafhankelijkheidsverklaring).

Verifieerbaar certificatieproces
EBN Certification hanteert een verifieerbaar certificatieproces. Voorafgaand aan het certificatieproces wordt de te certificeren onderneming geïnformeerd over de werkwijze van EBN Certification (bijlage V7, voorwaarden certificering). Vervolgens is elke stap die wordt gezet in het proces om te komen tot de beslissing om wel of geen certificaat af te geven, te verifiëren (bijlage V8, flow-chart audit). Als laatste stap in het proces wordt gecontroleerd of de juiste stappen zijn gezet. Dit gebeurt door een onafhankelijk opererende certificatiebeslisser voor wie het audit-rapport dus slechts als een advies dient.

Risico-inventarisatie (RIE) op het gebied van onafhankelijkheid en onpartijdigheid
EBN Certification beschikt over een op haar onafhankelijkheid en onpartijdigheid gerichte risico-inventarisatie (RIE). De RIE van EBN Certification wordt jaarlijks door de CvO en door de RvA beoordeeld. Ook is de RIE onderdeel van het interne auditproces van EBN Certification; het proces waarin EBN Certification haar processen door een externe partij laat auditeren.

Financieel onafhankelijk
EBN Certification heeft geen financiële banden met derden en is financieel onafhankelijk. Zij is, al jaren, in staat om zichzelf te bedruipen en heeft een gezonde financiële positie.

Belangenconflicten (12.2 Guidelines)
Het uitvoeren van haar taken door EBN Certification leidt niet tot een belangenverstrengeling. Dit blijkt onder andere uit de hierboven bedoelde RIE. In de RIE komen de risico's op belangenverstrengeling aan de orde en mede op basis daarvan zijn meerdere beheersmaatregelen genomen.

Zo is er een Handboek Auditor opgesteld waarin o.a. is opgenomen dat auditoren niet langer dan 6 jaar bij een organisatie betrokken mogen zijn als lead-auditor. Ook wordt jaarlijks een analyse uitgevoerd op de zittingsduur van auditoren en komt die analyse aan de orde bij de CvO. Voorts onthoudt EBN Certification zich van elke actie die niet met haar taken en verplichtingen verenigbaar is. Dit blijkt o.a. uit het feit:

- dat EBN Certification geen fees betaalt aan adviesbureaus voor het aanbrengen van klanten;
- dat financiële transacties door auditoren met consultancy bureaus niet zijn toegestaan;
- dat EBN Certification geen zaken doet met consultancybureaus of ZZP-ers die druk uitoefenen op de onpartijdigheid;
- dat EBN Certification geen zaken doet met adviesbureaus of ZZP-ers die uitingen doen waardoor een opdrachtgever in de veronderstelling kan komen dat er sprake is van een voorkeurspositie;
- dat er uitsluitend inhuur/inleen-contracten voor certificatiewerkzaamheden (o.a. auditwerkzaamheden) worden afgesloten met individuen;
- dat een auditor die een rol speelt in het certificatieproces geen advieswerk mag verrichten en geen interne audits mag uitvoeren en niet mag hebben uitgevoerd in afgelopen 2 jaar; hetgeen zij bij elke audit-opdracht ook schriftelijk verklaren;
- dat elke bij de audit betrokken externe adviesorganisatie expliciet wordt genoemd in het audit-rapport;
- dat een auditor niet is betrokken in het offertetraject en heeft geen financieel voordeel bij het al of niet behalen van certificatie door een klant;
- dat het personeel van EBN Certification is gebonden aan een gedragscode die gericht is op ethisch handelen en aan een geheimhoudingsplicht;
- dat alle auditoren per audit telkens opnieuw verklaren onafhankelijk te zijn;
- dat een certificatie-beslisser opereert onafhankelijk en kan dus niet onder druk worden gezet;
- dat de beslissing om wel of geen certificaat af te geven staat los van het facturatieproces.

Deskundigheid (12.3 Guidelines)
EBN Certification beschikt over het vereiste expertiseniveau om haar rol effectief te kunnen uitvoeren. Dit blijkt uit hoofdstuk 7 van richtlijn ISO/IEC 17021-1:2015 waarin is opgenomen aan welke algemene eisen een auditor moet voldoen. Daarnaast geldt dat elke auditor aantoonbaar kennis dient te hebben van de regels die gelden voor de bescherming van persoonsgegevens

(AVG) in relatie tot de sector van ISPS-bedrijven. Bij het indienen van dit verzoekschrift is een concreet competentieprofiel nog in ontwikkeling.

Vastgestelde procedure en structuren (12.4 Guidelines)
EBN Certification beschikt over een passende organisatiestructuur en over geschikte procedures en protocollen om toezicht te kunnen houden op de naleving van de Gedragscode en (dus) om adequaat te kunnen beoordelen of een organisatie in aanmerking komt om aan te sluiten en of de Gedragscode juist wordt toegepast.

Organisatie EBN Certification
EBN Certification heeft adequate bronnen en voldoende middelen en personeel om haar taken zorgvuldig en op gepaste wijze te kunnen uitvoeren; passend bij het verwachte aantal leden van de code en de omvang van die leden en de complexiteit of de mate van risico bij de verwerkingen. Dit blijkt uit het feit dat EBN Certification sinds jaar en dag voor de meest uiteenlopende bedrijven, branches en sectoren fungeert als certificerende instelling (zie ‘algemeen’ en ‘onafhankelijkheid’).

Certificatieprocedure (audits aan de hand van het certificatieschema)
Uit de voorgaande paragrafen volgt reeds dat EBN Certification vele protocollen heeft opgesteld om haar onafhankelijkheid te borgen en haar taken op de juiste wijze uit te voeren. De belangrijkste procedure waarmee EBN Certification vorm en inhoud geeft aan haar taken als toezichthoudend orgaan ten aanzien van de Gedragscode betreft het proces op basis waarvan een certificaat wordt verleend: de certificatieprocedure.

Het belangrijkste onderdeel van deze procedure betreft de audit. Tijdens een audit wordt de naleving van de gedragsregels getoetst aan de hand van een op te stellen certificatieschema om zo tot een auditrapport te komen. Een audit vindt plaats voorafgaand aan de aansluiting en vervolgens jaarlijks.

Sanctionerende maatregelen
EBN Certification stelt een effectieve procedure op om maatregelen te kunnen nemen tegen deelnemers die handelen in strijd met de Gedragscode, zoals een schorsing of uitsluiting van deelname aan Gedragscode.

Transparante klachtenbehandeling (12.5 Guidelines)
EBN Certification heeft een effectieve procedure om klachten te behandelen op een onpartijdige en transparante manier (bijlage V9, klachtenprotocol).

Communicatie met de AP (12.6 Guidelines)
Het toezichtmodel van EBN Certification maakt dat EBN Certification, indien nodig, goed in staat is om, zonder belemmeringen op te werpen of nadeel te veroorzaken, te communiceren met de AP en/of andere toezichthouders en/of overheden, bijvoorbeeld over audits of genomen maatregelen na overtredingen.

Beoordelingsmechanisme (12.7 Guidelines)
De Gedragscode voorziet in een beoordelingsmechanisme om er voor te zorgen dat de Gedragscode relevant blijft (zie Hoofdstuk 20 van de Gedragscode).

Juridische status (12.8 Guidelines)
Uit al het vorenstaande mag blijken dat EBN Certification de juiste statuur heeft om haar rol ex art. 41 lid 4 AVG te vervullen.

Toelichting
Uiteraard is Port Privacy graag bereid om haar verzoek mondeling en/of met stukken, nader te onderbouwen en/of toe te lichten. Ditzelfde geldt voor EBN Certification. Ook EBN Certification is in staat en bereid tot een nadere onderbouwing en/of toelichting van hetgeen over haar bedrijf wordt aangevoerd.

Conclusie en verzoek
Port Privacy komt tot de conclusie dat EBN Certification voldoet aan de eisen die de AVG en de Guidelines stellen aan een toezichthoudend orgaan en verzoekt de AP dan ook om EBN Certification te accrediteren om te kunnen fungeren als extern toezichthoudend orgaan ten behoeve van de Privacy Gedragscode voor het toegangsbeleid van ISPS-bedrijven in Nederland.

Ondertekening

Schiedam, 17 september 2019

_____
Port Privacy B.V.
mr. T.H. Poot

PORT PRIVACY

Bijlage V1 - Getekende verklaringen

PORT PRIVACY

Bijlage V2 - EBN - Bewijs van accreditatie door RvA

PORT PRIVACY

Bijlage V3 - EBN - Agenda CVO

PORT PRIVACY

Bijlage V4 - EBN - Gedragscode Personeel

PORT PRIVACY

Bijlage V5 - EBN - Geheimhoudingsverklaring Personeel

PORT PRIVACY

Bijlage V6 - EBN – Werkorder

PORT PRIVACY

Bijlage V7 - EBN - Voorwaarden voor Certificering

PORT PRIVACY

Bijlage V8 - EBN - Flowchart audit

PORT PRIVACY

Bijlage V9 - EBN - Klachtenreglement