CONSIDERATI

Legal partners in a digital world

Privacy en AIS in de binnenvaart

Ministerie van Infrastructuur en Milieu

9 mei 2017

mr. drs. Dominique Hagenauw
(hagenauw@considerati.com)
mr. Eva Heeger (heeger@considerati.com)

Privacy

IT law

Public affairs

CONSIDERATI
Legal partners in a digital world

Inhoudsopgave

1 INLEIDING 4

1.1 METHODOLOGIE 4

2 AIS-GEGEVENS 5

2.1 TECHNISCHE BESCHRIJVING AIS 5
2.2 ACHTERGROND EN DOEL GEBRUIK AIS 6
2.3 WELKE GEGEVENS ZIJN HIERBIJ BETROKKEN? 8

3 WET BESCHERMING PERSOONSGEGEVENS 10

3.1 DE WET BESCHERMING PERSOONSGEGEVENS 10
3.2 BEGRIPPEN EN DEFINITIES 10
Reikwijdte 11
Rechtsgrondslagen 12
Materiële eisen 13
Verantwoordelijke / bewerker 16

4 VERWERKING VAN AIS-GEGEVENS 17

4.1 ZIJN AIS-GEGEVENS PERSOONSGEGEVENS? 17
4.2 VERPLICHTE UITZENDING AIS GEGEVENS 18
4.3 ONTVANGERS VAN AIS-GEGEVENS 18
4.3.1 Vaarwegbeheerders 19
Kustwacht 21
Overige vaarwegbeheerders 22
4.3.2 Doelen en grondslagen voor de gegevensverwerking door de vaarwegbeheerders 22
4.4 OVERIGE ORGANISATIES 22
4.4.1 Doelen en grondslagen voor de gegevensverwerking door overige organisaties 23

5. VERDERE VERWERKING VAN AIS-GEGEVENS DOOR VAARWEGBEHEERDERS 24

5.1 ZEGGENSCHAP OVER AIS-GEGEVENS 24
5.2 PRIMAIR DOEL AIS: VERKEERSMANAGEMENT DOOR VAARWEGBEHEERDERS 25
Verenigbaar of onverenigbaar doel 26
5.3 GEBRUIK AIS-GEGEVENS VOOR VERKEERSMANAGEMENT 27
Operationeel beheer 28
Historisch beheer 29
5.4 VERSTREKKEN VAN AIS-GEGEVENS AAN PUBLIEKE PARTIJEN 30
Aan andere vaarwegbeheerders 30
Toezicht en handhaving 32
5.5 VERSTREKKEN VAN AIS-GEGEVENS AAN PRIVATE PARTIJEN 32
CBS, TNO & studenten 32
Havenbedrijf 33
Websites en apps 33
5.6 RELATIE MET DE 'OPEN DATA'-VERPLICHTING 34
5.7 VERANTWOORDELIJKHEID BIJ AANBESTEDINGEN 34

6. VERDERE VERWERKING VAN AIS-GEGEVENS DOOR ANDERE PARTIJEN DAN VAARWEGBEHEERDERS 35

Havenbedrijf 35

Vaarwegbeheerders *36*
Overige partijen *36*

7. ONTWIKKELINGEN 37

7.1 UITBREIDING LIJST VERPLICHT UIT TE ZENDEN INFORMATIE VIA DE AIS 37
7.2 TOEGANG TOT AIS-GEGEVENS VOOR TRANSPORTEURS 37
7.3 GEGEVENSVERWERKING DOOR ILT 37
7.4 GEZAMENLIJKE WALINFRASTRUCTUUR 38

8. ANALYSE PRIVACYVRAAGSTUKKEN AIS 40

9. CONCLUSIE 42

Gebruik door vaarwegbeheerders *42*
Gebruik door derden *43*
9.1 AANBEVELINGEN 44
Technisch *44*
Organisatorisch *44*
Handhaving *44*

1 Inleiding

Het directoraat-generaal Bereikbaarheid van het ministerie van Infrastructuur en Milieu (hierna DGB van het ministerie van I&M) heeft vernomen dat er signalen zijn dat binnenvaartschippers privacy-zorgen hebben ten aanzien van het gebruik van de signalen die worden uitgezonden door het Automatische Identificatie Systeem (AIS) dat door binnenvaartschepen moet worden uitgezonden.

Daarom heeft het DGB van het ministerie van I&M aan Considerati gevraagd een onderzoek te doen naar het gebruik van de AIS-informatie en naar de mogelijke schendingen van de privacy als gevolg van dit gebruik, zowel door vaarwegbeheerders als door ander partijen.

Het DGB van het ministerie van I&M wil allereerst weten in hoeverre er sprake is van schending van de privacy indien deze gegevens worden doorgegeven en bijvoorbeeld gepubliceerd worden op internet?

Daarnaast wil het DGB van het ministerie van I&M weten in hoeverre deze gegevens door de vaarwegbeheerders (en wellicht anderen) nog voor andere niet in de wet gespecificeerde doelen worden gebruikt. In hoeverre worden deze gegevens doorgegeven aan derden, voor welke doelen en met welke grondslag? En is daarbij voldoende gewaarborgd dat de gegevens niet voor andere doelen worden gebruikt?

1.1 Methodologie

Het onderzoek is gebaseerd op een *desk research* waarbij de documenten die door het DGB van het ministerie van I&M zijn aangeleverd, zijn bestudeerd. Ook is gebruik gemaakt van overige relevante bronnen die publiek beschikbaar zijn. Daarnaast zijn er interviews gehouden met medewerkers van relevante organisaties en met medewerkers van afdelingen binnen DGB en de Rijkswaterstaat (RWS).[1] Op basis van de informatie die hierin naar voren is gekomen, is dit rapport opgesteld.

In het tweede hoofdstuk wordt uitgelegd wat AIS precies inhoudt, hoe het AIS systeem werkt, waarvoor AIS wordt gebruikt en welke gegevens hierbij betrokken zijn. Daarna worden de meest relevante bepalingen van de Wbp en waar relevant de aankomende Algemene verordening gegevensbescherming (Avg) behandeld. Vervolgens wordt ingegaan op het verwerken van AIS-gegevens door de verschillende partijen. Bij deze partijen wordt onderscheid gemaakt tussen de vaarwegbeheerders en overige partijen. In de daaropvolgende twee hoofdstukken wordt dit onderscheid vastgehouden en wordt de verdere verwerking van de gegevens door deze partijen behandeld. In hoofdstuk zeven wordt ingegaan op de ontwikkelingen in het kader van AIS, waarna in het achtste hoofdstuk een analyse van de vraagstukken wordt gemaakt. Uiteindelijk wordt in het laatste hoofdstuk een conclusie wordt getrokken. In de conclusie wordt ingegaan op de risico's die gevonden zijn en worden aanbevelingen gedaan hoe deze risico’s geadresseerd kunnen worden.

[1] Rijkswaterstaat (diverse afdelingen), ministerie van Infrastructuur en Milieu (DGB), Binnenvaart, BLN-Schuttevaar en de Inspectie Leefomgeving en Transport (ILT).

2 AIS-gegevens

Voordat kan worden ingegaan op de vraag in hoeverre het gebruik van AIS een schending van de privacy inhoudt, is het belangrijk om uiteen te zetten wat AIS is en hoe het systeem werkt, waarvoor AIS wordt gebruikt en welke gegevens hierbij betrokken zijn.

2.1 Technische beschrijving AIS

Het Automatische Identificatie Systeem, oftewel AIS, is een technologie waarmee schippers met elkaar en met systemen die aan de walkant zijn geplaatst, communiceren. Met behulp van een VHF-zender zenden AIS-apparaten automatisch en met regelmatige tussenpozen de relevante informatie uit door middel van radiogolven. Met een VHF-ontvanger, die is afgestemd op de juiste frequentie(s) en die is uitgerust om de digitale AIS berichten te decoderen, kunnen de radiogolven, en daarmee dus de informatie die hiermee wordt verstuurd, worden opgevangen.

Er kan onderscheid worden gemaakt tussen de volgende communicatievormen[2]:

- Tussen schepen onderling: alle schepen die met AIS zijn uitgerust, wisselen statische en dynamische informatie uit met alle AIS-schepen binnen radiobereik;
- Tussen schepen en de wal: data van AIS-schepen worden ontvangen door AIS-stations aan wal die kunnen verbonden zijn met een centraal systeem, bijvoorbeeld een RIS-centrum[3];
- Tussen de wal en schepen: gegevens die relevant zijn voor de veiligheid kunnen van de wal naar schepen worden verzonden.

Een AIS-apparaat zendt een radiosignaal uit[4] en wordt daarmee gezien als een vorm van marifonie.[5] Daarom kan AIS worden beschouwd als een elektronisch communicatienetwerk in de zin van artikel 1(e) van de Telecommunicatiewet.[6] De schipper is dan ook verplicht om het apparaat aan te melden bij het Agentschap Telecom, dat de frequentie toewijst en erop toeziet dat radiozendapparaten de juiste identificaties uitzenden.[7]

Afhankelijk van het vaargebied, moet het AIS-apparaat permanent ingeschakeld zijn, behoudens enkele uitzonderingen. Bovendien moeten de ingevoerde gegevens op ieder moment met de werkelijke gegevens van het schip overeenkomen.[8]

---

[2] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32007R0415.
[3] RIS staat voor River Information Service, zie paragraaf 2.2. Een RIS-centrum is de plaats waar de informatiediensten door RIS-personeel worden aangestuurd, volgens *Richtlijnen en aanbevelingen voor River Information Services) (RIS Guidelines 2002)*, 2003, p. 6. Raadpleegbaar via: https://www.ccr-zkr.org/files/documents/ris/guidelines20_nl.pdf.
[4] Art. 4 lid 5 Richtlijn 2005/44/EG juncto 2000/637/EG: Beschikking van de Commissie van 22 september 2000 over de toepassing van artikel 3, lid 3, onder e), van Richtlijn 1999/5/EG van het Europees Parlement en de Raad op radioapparatuur die onder de regionale regeling betreffende de radiotelefoondienst op binnenwateren valt (kennisgeving geschied onder nummer C(2000) 2718) (Regionale Regeling betreffende de radiotelefoondienst op binnenwateren).
[5] https://www.vaarbewijzen.nl/ais.html.
[6] Art. 1 sub e Telecommunicatiewet.
[7] https://www.agentschaptelecom.nl/onderwerpen/scheepvaart/maritieme-radiozendapparatuur/ais-volgsysteem-voor-de-scheepvaart.
[8] Art. 4.07 lid 2 Binnenvaartpolitiereglement.

2.2 Achtergrond en doel gebruik AIS

In de zeevaart wordt AIS al sinds 2003 gebruikt om ervoor te zorgen dat zeeschepen elkaar kunnen identificeren, met elkaar kunnen communiceren en hun locatie kunnen uitwisselen, met als doel de veiligheid op het water te vergroten. De toepassing van AIS in de binnenvaart is een keuze van de vaarwegbeheerder, die besluit automatisch melden en volgen op de vaarweg in te voeren. Het gevolg van dit besluit van de vaarwegbeheerder is dat hij verplicht is daarvoor inland AIS te gebruiken zoals is voorgeschreven door de EU verordeningen 415/2007 en 689/2010 die een bijlage zijn van de EU RIS richtlijn 2005/44 EG. Hoewel deze Richtlijn AIS niet verplicht voorschrijft, heeft de wetgever bij de implementatie van de wet voor dit systeem gekozen. De Richtlijn levert een belangrijke bijdrage aan het verbeteren van de veiligheid, doeltreffendheid en milieuvriendelijkheid van binnenwateren in de EU.[9]

RIS hebben geen betrekking op interne commerciële activiteiten tussen een of meer betrokken bedrijven, maar kunnen volgens de RIS Richtlijn wel aan commerciële activiteiten worden gekoppeld. De RIS Richtlijn beschrijft echter niet tot in detail wat er met commerciële activiteiten wordt bedoeld, wel wordt genoemd dat RIS diensten als vaarweginformatie, verkeersinformatie, verkeersbeheer, ondersteuning van calamiteitenbestrijding, informatie voor vervoersmanagement, statistieken en douanediensten en waterwegheffingen en havengelden omvat.[10]

De RIS-Richtlijn vereist dat de RIS-systemen doeltreffend zijn. Bovendien moeten de systemen uit te breiden zijn en moeten zij interoperabel zijn, zodat ze aan andere RIS-toepassingen en eventueel aan systemen voor andere vervoerswijzen, vervoerssystemen en commerciële activiteiten kunnen worden gekoppeld.[11]

Tijdens de Nederlandse implementatie van deze Richtlijn zijn twee technologieën overwogen om te gebruiken om te voldoen aan de verplichtingen uit de RIS Richtlijn:

- Automatische Identificatie met Internet Protocol (AI-IP): Schepen communiceren met elkaar en met de walkant via een mobiel netwerk.
- Automatic Information Systems (AIS): Schepen communiceren met elkaar en met de walkant via radiogolven die door een VHF-zender wordt uitgezonden (de zogenoemde *peer to peer* technologie).

Uiteindelijk is er in 2006 voor gekozen om AIS-apparatuur te gebruiken, zoals ook in de kamerbrief van 18 augustus 2010 is toegelicht. De keuze is ook vastgelegd in het Convenant binnenvaart van 14 november 2006. Nadien is Verordening 415/2007 gepubliceerd, waarin inland AIS als het te gebruiken systeem is vastgelegd.

[9] Art. 1 lid 1 Richtlijn 2005/44/EC.
[10] Art. 3 sub a Richtlijn 2005/44/EC.
[11] Art. 4 lid 2 Richtlijn 2005/44/EC.

In de kamerbrief wordt aangegeven dat ten behoeve van de veiligheid ook de branchepartijen de keuze voor AIS te respecteren, ondanks de privacy bezwaren. Hierbij is wel afgesproken dat de informatie beperkt blijft tot de locatie en de naam van het schip.[12]

In tegenstelling tot systemen die via een mobiel netwerk met elkaar communiceren, worden radiosignalen namelijk niet aangetast als het netwerk niet meer werkt. Schepen kunnen met elkaar blijven communiceren ook in geval van storingen op het mobiele netwerk of de vaste infrastructuur. In de zeevaart had men bovendien goede ervaring met AIS en door AIS eveneens in de binnenvaart te gebruiken, kunnen zee- en binnenvaartschepen ook met elkaar communiceren. De keerzijde is dat AIS-signalen uitgezonden via een VHF-zender niet beveiligd of versleuteld zijn en daardoor voor iedereen met een geschikte ontvanger zijn te ontvangen.

In Nederland zijn de regels uit de Richtlijn omgezet door de Scheepvaartverkeerswet te wijzigen.[13] In de Scheepvaartverkeerswet zijn de *River Information Services* gedefinieerd als de geharmoniseerde informatiediensten ter ondersteuning van het verkeers- en vervoersmanagement voor de binnenvaart, met inbegrip van de technisch haalbare koppelingen met andere vervoerswijzen dan wel met commerciële activiteiten, niet zijnde interne commerciële activiteiten tussen betrokken bedrijven.[14]

In het Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart uit 2012 is bevestigd dat in Nederland bepaald is door de vaarwegbeheerders dat AIS het systeem zal zijn waarmee invulling wordt gegeven aan de verplichtingen uit de RIS Richtlijn ten aanzien van verkeersmanagement. [15] Hierop heeft de Autoriteit Persoonsgegevens (voorheen het College bescherming persoonsgegevens) in januari 2012 geadviseerd, waarin hij onder andere heeft aangegeven dat de grondslag helderder geregeld moest worden en dat meer aandacht moest worden besteed aan de noodzaak en de uitzonderingen.[16] In mei 2012 is het Besluit vervolgens aangenomen.

De regels omtrent het gebruik van AIS in de binnenvaart zijn vervolgens neergelegd en verder uitgewerkt in artikel 4.07 van het Rijnvaartpolitiereglement, dat van toepassing is sinds 1 december 2014, en in artikel 4.07 van het Binnenvaartpolitiereglement, dat is ingegaan op 1 januari 2016.[17] [18] Er is voor gekozen dat enkel een bepaald type AIS-apparatuur is toegelaten, het zogenoemde Inland AIS-apparaat.[19]

---

[12] Brief van 18 augustus 2010 van de minister van Verkeer en Waterstaat aan de Tweede Kamer en het (verlopen) Convenant tussen het ministerie van Verkeer en Waterstaat en Koninklijke Schuttevaer, Kantoor Binnenvaart, Centraal Bureau voor de Riin- en Binnenvaart en de Vereniging van sleep- en duwbooteigenaren Rijn en IJssel.

[13] *Kamerstukken 2006/2007*, 30974, Wijziging Scheepvaartverkeerswet i.v.m. implementatie richtlijn nr. 2005/44/EG (geharmoniseerde River Information Services (RIS) binnenwateren Gemeenschap).
[14] Art. 1 lid 1 sub p Scheepvaartverkeerswet.
[15] http://wetten.overheid.nl/BWBR0031560/2015-06-01.
[16] Wetgevingsadvies CBP t.a.v. Besluit meldingsformaliteiten en gegevensverwerking scheepvaart.
[17] http://wetten.overheid.nl/BWBR0003628/2016-01-01 en http://wetten.overheid.nl/BWBR0006923/2016-12-01.

Net als in de zeevaart is het gebruik van AIS in de binnenvaart bedoeld om de verkeersveiligheid op de vaarwegen te vergroten. Schepen kunnen door middel van AIS makkelijker met elkaar maar ook met de walinfrastructuur van vaarwegbeheerders communiceren over de positie en identificatie van de schepen.

Tenslotte is het Privacyreglement verkeersregistratiesystemen Rijkswaterstaat relevant om te vermelden, aangezien hierin sinds juli 2003 beleidsregels zijn vastgesteld ten aanzien van privacy en verkeersregistratiesystemen.[20]

2.3 Welke gegevens zijn hierbij betrokken?

In de RIS Richtlijn is niet vastgelegd welke gegevens door AIS-apparaten moeten worden uitgezonden. Wel wordt in de Verordening 415/2007 van de Europese Unie inzake de technische specificaties voor tracking- en tracingsystemen voor schepen, aangevuld met Uitvoeringsverordening 689/2012, overeenkomstig artikel 5 van de RIS Richtlijn bepaald dat AIS-berichten in ieder geval de volgende informatie dienen te bevatten: [21]

- Statische informatie, zoals het officiële scheepsnummer, de roepnaam van het schip, de naam van het schip en het scheepstype;
- Dynamische gegevens, zoals de positie van het schip met een indicatie van de nauwkeurigheid en de integriteitstatus;
- Reisgerelateerde informatie, zoals de lengte en grootste breedte van het schip/scheepssamenstel en informatie over eventuele gevaarlijke lading aan boord;
- Specifieke binnenvaartinformatie, zoals het de geschatte tijd van aankomst bij een sluis/brug/terminal/grens.

Statische informatie is dus die informatie die niet gewijzigd kan worden en die verbonden is aan het gebruikte AIS-apparaat en het schip. Dynamische informatie betreft de gegevens die wijzigen door verplaatsing van het schip, maar ook informatie die door de schipper aangepast kan worden en volgens de wet zelfs aangepast moet worden om ervoor te zorgen dat de informatie over het schip correct zijn. Bovendien kunnen korte, op de veiligheid betrekking hebbende tekstberichten, worden uitgewisseld tussen schepen onderling en tussen het schip en de walzijde.[22]

In de Verordening 415/2007 wordt nog nader op de technische details ingegaan. In Nederland is in artikel 4.07 lid 3 van het Binnenvaartpolitiereglement vastgelegd welke gegevens tenminste moeten worden verstuurd via het AIS-signaal. Dit zijn:[23]

- User Identifier (Maritime Mobile Service Identity (MMSI), Radio Call Sign);
- naam van het schip;

---

[18] https://www.rijkswaterstaat.nl/over-ons/nieuws/nieuwsarchief/p2016/04/politie-rijkswaterstaat-en-havenbedrijven-gaan-ais-plicht-vanaf-1-mei-handhaven.aspx.
[19] https://www.rijkswaterstaat.nl/over-ons/nieuws/nieuwsarchief/p2014/11/Praktische-folder-Rijkswaterstaat-over-verplichtst.aspx.
[20] http://wetten.overheid.nl/BWBR0015302/2003-07-11.
[21] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32007R0415.
[22] Centrale Commissie voor de Rijnvaart, *Informatieblad Inland AIS,* Editie 2011, p. 11-12.
[23] Art. 4.07 lid 3 Binnenvaartpolitiereglement.

- scheeps- of samensteltype;
- uniek Europees scheepsidentificatienummer (ENI);
- lengte over alles van het schip of het samenstel met een nauwkeurigheid van 0.1 meter;
- breedte over alles van het schip of het samenstel met een nauwkeurigheid van 0.1meter;
- positie;
- snelheid over de grond;
- koers over de grond;
- tijd van elektronische positiebepaling;
- vaarstatus;
- referentiepunt voor de positie-informatie op het schip met de nauwkeurigheid van 1 meter.

Een schipper kan ervoor kiezen om meer gegevens te versturen via de AIS-radiogolven, bijvoorbeeld informatie over de lading die hij vervoert.

3 Wet bescherming persoonsgegevens

Alvorens wordt ingegaan op de privacyaspecten van AIS, wordt eerst het juridisch kader voor privacy uiteengezet. Het belangrijkste stuk wetgeving dat van toepassing is op voornoemde vragen is de Wet bescherming persoonsgegevens (Wbp). Vanaf mei 2018 zal de Algemene Verordening Gegevensverordening (Avg of Verordening) de huidige privacywetgeving vervangen. Hoewel de Avg thans nog niet van toepassing is, zullen in deze rapportage, waar relevant, de toekomstige eisen worden genoemd.

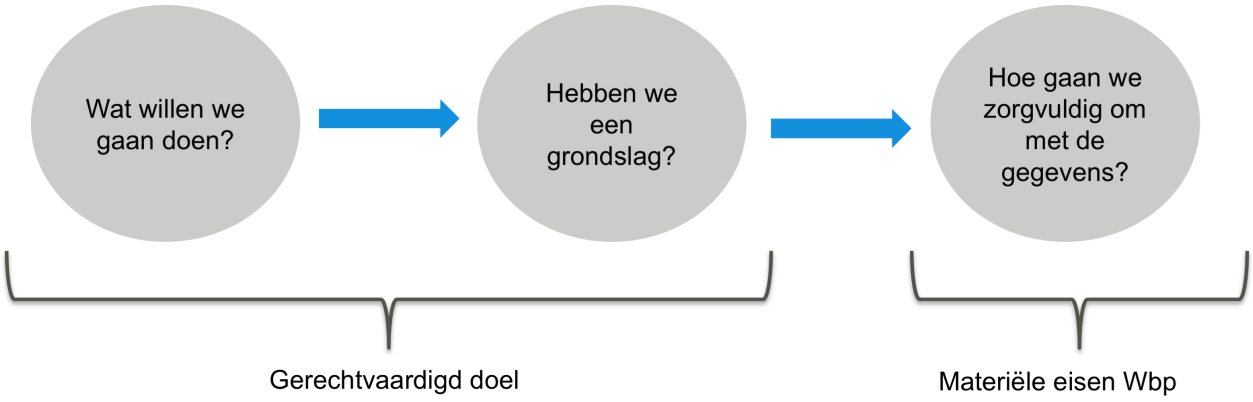
3.1 De Wet bescherming persoonsgegevens

De Wbp bepaalt wanneer een natuurlijke persoon of een rechtspersoon (de verantwoordelijke) persoonsgegevens mag verwerken.

Kern van de wet is dat persoonsgegevens alleen mogen worden verwerkt voor nadrukkelijk omschreven en gerechtvaardigde doeleinden. Een doel is gerechtvaardigd als het gebaseerd kan worden op één van de grondslagen uit artikel 8 Wbp.

Wanneer er een gerechtvaardigd doel is, dan mogen gegevens verwerkt worden. Bij het verwerken van persoonsgegevens zelf moet vervolgens voldaan worden aan de materiële eisen uit de Wbp. Het gaat dan om zaken als adequate beveiliging, transparantie en het invulling geven aan de rechten van de betrokkene.

Schematisch kan de logica van de Wbp als volgt worden weergegeven:



3.2 Begrippen en definities

In dit hoofdstuk worden de voor AIS relevante juridische aspecten behandeld, waarbij onderscheid wordt gemaakt tussen de reikwijdte, dus wanneer de wet van toepassing is, de rechtsgrondslagen, de materiële normen en de begrippen ‘verantwoordelijke’ en ‘bewerker’.

Reikwijdte

De Wbp (en straks ook de Avg) is van toepassing op alle verwerkingen van persoonsgegevens die in Nederland (en straks in de EU) plaatsvinden. De twee relevante elementen, 'verwerken' en 'persoonsgegevens', zullen hieronder worden uiteengezet.

Verwerken

'Verwerken' betreft alle handelingen die men met persoonsgegevens kan verrichten. De Wbp zelf geeft een ruime, niet-uitputtende omschrijving van handelingen die onder het begrip verwerking vallen:

"(....) in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens."[24]

Het *verstrekken* van persoonsgegevens is óók een verwerking en mag dus alleen geschieden als daar een specifieke rechtmatige grondslag voor is. Gegevens mogen aan derden worden verstrekt als daar een verwerkingsgrondslag voor is te vinden. Of een verwerking noodzakelijk is, hangt af van de omstandigheden van het geval. Dit is ter beoordeling aan de verantwoordelijke.

Persoonsgegevens

Een 'persoonsgegeven' wordt in de wet gedefinieerd als *'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'*.[25] Zodra een persoon dus direct of indirect te identificeren is, zijn de gegevens persoonsgegevens en moeten deze worden verwerkt volgens de Wbp.

Een persoon wordt als identificeerbaar beschouwd indien hij direct of indirect kan worden geïdentificeerd aan de hand van één of meerdere gegevens, bijvoorbeeld de geboortedatum, woonplaats of een *online*-identificator. Deze gegevens zijn dan ook persoonsgegevens. Om te spreken van identificeerbaarheid is het niet noodzakelijk dat de naam van de persoon ook bekend is. Als iemand uniek kan worden onderscheiden in een groep mensen, dan is deze persoon identificeerbaar en zijn de gegevens persoonsgegevens.[26] Dit wordt in de Avg bij wet vastgelegd.[27]

Dit houdt in dat zowel gegevens die direct over een persoon gaan, als gegevens die naar een natuurlijk persoon te herleiden zijn, binnen de reikwijdte van de Wbp vallen. Grofweg kan men ervan uit gaan dat alle gegevens die op een levend persoon betrekking hebben en het mogelijk maken om deze persoon (indirect) te identificeren – dan wel uniek te onderscheiden van andere personen – persoonsgegevens zijn.[28]

---

[24] Artikel 1sub b Wbp.
[25] Artikel 1sub a Wbp.
[26] Zie hiervoor: Artikel 29 Werkgroep (2007), Opinion 4/2007 on the Concept of Personal Data.
[27] Overweging 26 Avg.
[28] Zie hiervoor: Artikel 29 Werkgroep (2007), Opinion 4/2007 on the Concept of Personal Data.

- Gevoelige gegevens

Een aantal persoonsgegevens wordt aangemerkt als gevoelige gegevens. Dit zijn niet per se bijzondere persoonsgegevens (zie hiervoor de volgende paragraaf), maar betreffen gegevens die als gevoelig ervaren worden door betrokkenen. Dit zijn bijvoorbeeld financiële gegevens, locatiegegevens of gegevens over surfgedrag.[29]

Voor het verwerken van deze persoonsgegevens is het belangrijk om extra waarborgen te treffen om te garanderen dat ze in overeenstemming met de wet worden verwerkt.

Hoe gevoeliger de gegevens namelijk zijn voor de betrokkene, hoe minder snel mag worden aangenomen dat deze gegevens bijvoorbeeld ook voor andere doeleinden mogen worden gebruikt en hoe meer reden er is de betrokkene gedetailleerder te informeren over de gegevensverwekingen. Ook geldt over het algemeen dat hoe gevoeliger de gegevens zijn, hoe zwaarder de getroffen beveiligingsmaatregelen moeten zijn.

- Bijzondere categorieën persoonsgegevens

Voor het verwerken van bijzondere categorieën persoonsgegevens geldt een verwerkingsverbod, met daarop uitzonderingen zoals de expliciete toestemming van een betrokkene. Als bijzondere persoonsgegevens worden gegevens aangemerkt die betrekking hebben op iemands godsdienst, ras, gezondheid, seksuele leven, politieke voorkeur of gegevens over hinderlijk, onrechtmatig of strafbaar gedrag.[30] De Avg breidt deze lijst uit met biometrische en genetische gegevens.[31]

De reden voor dit strengere regime is gelegen in het feit dat de verwerking van bijzondere persoonsgegevens in potentie een grotere bedreiging vormt voor de persoonlijke levenssfeer van de betrokkenen.

Rechtsgrondslagen

De Wbp bepaalt dat persoonsgegevens alleen mogen worden verwerkt als hiervoor een rechtsgrondslag bestaat. Er zijn zes mogelijke gronden op basis waarvan gegevens verwerkt mogen worden. Dit zijn:

- **Toestemming**; persoonsgegevens kunnen worden verwerkt als de betrokkene ondubbelzinnige toestemming heeft geven voor de verwerking. Toestemming betekent elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. De betrokkene moet de toestemming te allen tijde kunnen intrekken.
    - Bijvoorbeeld voor het verwerken van persoonlijke informatie en voorkeuren om meer gepersonaliseerde dienstverlening te bieden.

- **Uitvoering van een contract**; persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is. Ook mogen persoonsgegevens worden verwerkt om precontractuele

[29] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/reclame-en-profilering/profilering.
[30] Artikel 16 Wbp.
[31] Artikel 9 Avg.

maatregelen te nemen naar aanleiding van een verzoek van de betrokkene en als deze noodzakelijk zijn voor het sluiten van de overeenkomst.
    - Bijvoorbeeld het rekeningnummer in het kader van een koopcontract.

- **Wettelijke plicht**; gegevens mogen worden verwerkt indien dit noodzakelijk is om een wettelijke plicht na te komen.
    - Bijvoorbeeld voor het kunnen voldoen aan de eisen van de Belastingwetgeving.

- **Vitaal belang**; gegevens mogen worden verwerkt als dit noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene. Om deze rechtsgrondslag te kunnen gebruiken, moet het gaan om een zaak van leven of dood.
    - Bijvoorbeeld bij een ernstig ongeval, waarbij de persoon niet aanspreekbaar is, om de juiste hulp te kunnen verlenen.

- **Publiekrechtelijke taak;** gegevens mogen worden verwerkt als dit noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt.
    - Bijvoorbeeld het verwerken van gegevens door de gemeente ten behoeve van de Basisregistratie personen.

- **Gerechtvaardigd belang**; gegevens kunnen worden verwerkt als dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op de bescherming van de persoonlijke levenssfeer, prevaleert. Betrokkenen hebben altijd het recht om verzet aan te tekenen tegen verwerkingen die op basis van het gerechtvaardigd belang plaatsvinden. Onder de Avg is het niet langer mogelijk voor publieke organisaties om gegevensverwerkingen op deze rechtsgrondslag te baseren.[32]
    - Bijvoorbeeld direct marketing door de verantwoordelijke aan zijn eigen klanten.

Elke verwerking van persoonsgegevens, waaronder de doorgifte van gegevens, moet gebaseerd zijn op één van deze rechtsgrondslagen. Wanneer dat niet het geval is, mogen de persoonsgegevens niet worden verwerkt.

Materiële eisen

Op het moment dat bepaald is dat de Wbp van toepassing is en dat er een rechtsgrondslag is voor de verwerking van persoonsgegevens, zal ook moeten worden voldaan aan de materiële eisen van de wet. Hieronder worden de meest relevante materiële eisen behandeld.

[32] Artikel 6 lid 1 onder f, laatste zin, Avg.

Doelbinding

Gegevens mogen alleen verzameld worden voor een specifiek en gerechtvaardigd doel en mogen niet verder worden verwerkt voor andere doeleinden die niet verenigbaar zijn met dit oorspronkelijke doel. Per geval zal beoordeeld moeten worden of het nieuwe doel verenigbaar is met het oorspronkelijke doel van de verzameling. Bij deze afweging kunnen onder andere worden meegenomen hoe dicht deze doelen bij elkaar liggen, wat de redelijke verwachtingen van de betrokken zijn, de aard van de gegevens en welke risico-beperkende maatregelen zijn getroffen.

Dataminimalisatie

Er mogen niet meer persoonsgegevens worden verzameld dan noodzakelijk is voor het doel waarvoor ze worden verzameld. Dit betekent dat alle gegevens die worden verzameld ten behoeve van een bepaald doel toereikend, ter zake dienend en niet bovenmatig moeten zijn. Het is belangrijk om bij elke verwerking te bepalen of de gegevens nodig zijn om het doel te behalen, waarbij het uitgangspunt '*need to have*' moet zijn in plaats van '*nice to have*'.

Dataminimalisatie werkt ook in het voordeel van organisaties die persoonsgegevens verwerken. Immers, hoe minder gegevens worden verzameld, hoe lager het risico is voor de privacy van betrokkenen en het risico op non-compliance van de verantwoordelijke.

Bewaartermijnen

De Wbp bepaalt dat persoonsgegevens zo lang mogen worden bewaard als noodzakelijk voor het doel waarvoor ze zijn verzameld of vervolgens worden verwerkt, behoudens wettelijke plichten die een wettelijke bewaartermijn kunnen voorschrijven. [33] De verantwoordelijke bepaalt derhalve zelf hoe lang de persoonsgegevens bewaard dienen te worden. Daarbij dient goed afgewogen te worden hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt.

Beveiliging

Op basis van de Wbp is de verantwoordelijke verplicht om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. [34] Bij de beveiliging moet rekening worden gehouden met de fysieke beveiliging, de opslag van gegevens en de beveiliging van dataverkeer. De beveiligingsplicht strekt zich uit over het gehele proces van gegevensverwerking.

De beveiligingsmaatregelen dienen, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een passend beveiligingsniveau te garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. [35] Bij beveiligingsmaatregelen kan onder meer gedacht worden aan pseudonimisering, versleuteling van gegevens of het implementeren van beveiligingsstandaarden die de vertrouwelijkheid, integriteit en beschikbaarheid van de

[33] Artikel 10 Wbp.
[34] Artikel 13 Wbp.
[35] H. de Vries, Wet bescherming persoonsgegevens, in: P.C. Knol & G.J. Zwenne, Tekst & Commentaar Telecommunicatie- en privacyrecht, Wolters Kluwer: Deventer 2015, p. 890.

verwerkingssystemen garanderen. Hoe gevoeliger de gegevens zijn, hoe zwaarder de eisen die gesteld worden aan de beveiliging van de gegevens.

Wanneer er, ondanks de genomen maatregelen, een inbreuk op de beveiliging heeft plaatsgevonden en er is een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens naar aanleiding van het datalek, dan moet de verantwoordelijke onverwijld melding hiervan doen bij de Autoriteit Persoonsgegevens, uiterlijk binnen 72 uur. Wanneer een verantwoordelijke handelt in strijd met de meldplicht datalekken, kan de Autoriteit Persoonsgegevens een boete opleggen die op dit moment kan oplopen tot maximaal 820.000 euro. Onder de Avg kan deze boete oplopen tot 10 miljoen euro of 2% van de wereldwijde jaaromzet, indien dit laatste bedrag hoger is.[36]

Transparantie

Organisaties die persoonsgegevens verwerken, moeten transparant zijn over de verwerkingen die zij uitvoeren. De verantwoordelijke moet bijvoorbeeld de betrokkene informeren over zijn identiteit en hij moet aangeven hoe contact met hem kan worden opgenomen. Ook moet duidelijk worden gemaakt welke gegevens worden verwerkt en voor welke doeleinden de gegevens worden verwerkt. Daarnaast moet de verantwoordelijke alle overige informatie geven om te voldoen aan de eis van een behoorlijke en zorgvuldige verwerking van persoonsgegevens.

Onder de Verordening wordt het vereiste van transparantie duidelijker vastgelegd dan in het huidige wettelijke kader, door het als één van de basisbeginselen te benoemen waaraan verantwoordelijken moeten voldoen wanneer zij persoonsgegevens verwerken.

Rechten van de betrokkenen

Betrokkenen, dus de personen op wie de persoonsgegevens betrekking hebben, hebben op grond van de Wbp een aantal rechten ten opzichte van de verantwoordelijke. De betrokkene heeft ten eerste het recht op inzage in de gegevens die over hem worden verwerkt door de verantwoordelijke. De verantwoordelijke moet binnen vier weken reageren op het verzoek, waarbij een volledig overzicht van de verwerkte persoonsgegevens moet worden gegeven, de doeleinden waarvoor ze worden verwerkt en of ze aan anderen worden verstrekt.

De betrokkene heeft vervolgens ook het recht om de verantwoordelijke te verzoeken om de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, als de persoonsgegevens feitelijk onjuist zijn, niet volledig of niet relevant zijn. [37]

De Verordening voegt hier nog het recht op vergetelheid en het recht op gegevensoverdraagbaarheid aan toe. Het recht op vergetelheid is het recht van betrokkenen om te verzoeken om verwijdering van de persoonsgegevens, waarbij de verantwoordelijke de plicht heeft dit door te geven aan derden aan wie de gegevens zijn verstrekt.[38] Het recht op gegevensoverdraagbaarheid betekent dat een betrokkene zijn of haar gegevens van de ene organisatie moet kunnen meenemen naar een andere organisatie, indien de verwerking

[36] Artikel 83 lid 4 Avg.
[37] Artikel 35 en 36 Wbp.
[38] Artikel 17 Avg.

plaatsvond op basis van toestemming of op basis van het uitvoeren van een contract en wanneer dit technisch mogelijk is.[39]

De verantwoordelijke zal daarom processen en procedures moeten inrichten om uitvoering te kunnen geven aan de rechten van betrokkenen.

Verantwoordelijke / bewerker

De organisatie die het doel en de middelen van de gegevensverwerking bepaalt, is de verantwoordelijke in de zin van de Wbp. Degene die dus bepaalt welke persoonsgegevens moeten worden verwerkt, waarom en op welke manier, is de verantwoordelijke. Deze partij is er verantwoordelijk voor dat de verwerkingen van persoonsgegevens in overeenstemming met de wet geschieden.[40] Daarnaast is deze partij aanspreekpunt voor de betrokkenen en voor de toezichthouder.

De verantwoordelijke kan ervoor kiezen om bepaalde verwerkingen uit te besteden aan een derde partij. De partij die voor en/of namens de verantwoordelijk gegevens verwerkt, is de bewerker. Om te zorgen dat de verwerkingen die worden uitgevoerd door de bewerker ook in overeenstemming met de Wbp gebeuren, moet er een bewerkersovereenkomst worden getekend.

Het is hierbij belangrijk dat de bewerker zelf op geen enkele manier de persoonsgegevens verwerkt voor zijn eigen doeleinden. Zodra dit het geval is, zal de bewerker voor die verwerkingen zelf verantwoordelijke worden onder de Wbp en zal hij moeten voldoen aan de eisen uit de wet.

[39] Artikel 20 Avg.
[40] H. de Vries, *Wet bescherming persoonsgegevens,* in: P.C. Knol & G.J. Zwenne, *Tekst & Commentaar Telecommunicatie- en privacyrecht*, Wolters Kluwer: Deventer 2015, p. 857-858.

4 Verwerking van AIS-gegevens

Zoals uit het vorige hoofdstuk blijkt, is de Wbp van toepassing op het verwerken van persoonsgegevens. De Wbp is enkel van toepassing op AIS-gegevens als deze te kwalificeren zijn als persoonsgegevens. In dit hoofdstuk wordt daarom allereerst bepaald in hoeverre AIS-gegevens persoonsgegevens zijn. Daarna wordt ingegaan op de meest relevante vorm van verwerken, namelijk het verzamelen van deze gegevens.

4.1 Zijn AIS-gegevens persoonsgegevens?

AIS is een systeem dat in de zeevaart al langer wordt gebruikt en dat in verschillende stappen sinds 1 januari 2014 voor binnenvaartschepen verplicht is om te hebben en om hiermee continue gegevens uit te zenden.

Waar in het kader van de zeevaart nauwelijks tot geen privacy-gerelateerde zorgen bestaan, heeft DGB van het ministerie van I&M wel signalen ontvangen van privacy-zorgen bij binnenvaartschippers ten aanzien van het gebruik van AIS. Het verschil tussen de zeevaart en de binnenvaart is dat veel van de binnenschepen in eigendom zijn van familiebedrijven[41] of dat hierop schippers als ZZP-er werken.[42] Dit betekent dat voor veel binnenschippers het schip zowel hun werkplek als hun woning is.

Zoals in hoofdstuk 2 is beschreven, zendt het AIS-apparaat op een schip met regelmatige tussenpozen bepaalde gegevens uit, waaronder de unieke MMSI- en ENI nummers, de naam en de positie van het schip. Op basis van de MMSI- en ENI nummers kunnen schepen uniek worden onderscheiden en omdat het schip nauw verbonden is aan de schipper (en zijn gezin), zijn deze gegevens al snel aan te merken als persoonsgegevens.

Daarnaast zendt het AIS-apparaat continu de positie van het schip uit. Dit zijn locatiegegevens die door de Autoriteit Persoonsgegevens worden gezien als gevoelige gegevens, die met gepaste zorgvuldigheid behandeld moeten worden. Locatiegegevens kunnen namelijk iets zeggen over de routines en voorkeuren van een individu. Ook kunnen uit deze gegevens conclusies worden getrokken die een impact kunnen hebben op de persoonlijke levenssfeer van de betrokkene. Het verwerken van deze persoonsgegevens brengt daarom ook een verhoogd risico met zich mee.

Vanwege het feit dat een binnenvaartschip zo nauw, zo niet onlosmakelijk, is verbonden met de schipper zelf, zijn bepaalde gegevens die via AIS worden verzonden in de binnenvaart persoonsgegevens. De Autoriteit Persoonsgegevens (toen nog het College bescherming persoonsgegevens) heeft dit in haar wetgevingsadvies ten aanzien van de wijziging van de

[41] In 2009 waren meer dan de helft van de binnenschepen in eigendom van familiebedrijven, volgens http://repository.tudelft.nl/view/ir/uuid:ab6665b5-f69e-44d3-9bf5-50bffa3202ce/, p. 23.
[42] In 2011 opereerde ruim twee derde van de binnenschippers als ZZP'er of had slechts één werknemer volgens http://informatie.binnenvaart.nl/algemeen/de-binnenvaart/64-visie-op-transport-a-logistiek-2011.

Scheepvaartverkeerswet bevestigd.[43] Dit is ook door de Centrale Commissie voor de Rijnvaart en de Europese Unie erkend.[44]

4.2 Verplichte uitzending AIS gegevens

Op grond van artikel 4.07 lid 1 van het Binnenvaartpolitiereglement moet op een groot aantal vaarwegen in Nederland een schip uitgerust zijn met een AIS-apparaat**.** Er bestaan uitzonderingen op deze verplichting, bijvoorbeeld voor kleine schepen onder de 20 meter, hoewel ook deze schepen onder bepaalde omstandigheden weer wel met een AIS-apparaat moeten zijn uitgerust.

Het tweede lid van artikel 4.07 van het Binnenvaartpolitiereglement verplicht schepen om het AIS-apparaat permanent ingeschakeld te hebben. De gegevens die worden uitgezonden, moeten daarnaast op ieder moment overeenkomen met de correcte informatie op dat moment over het schip, zoals de lengte, breedte, herkomst en bestemming. De schipper is er verantwoordelijk voor dat deze informatie correct is en is er tevens verantwoordelijk voor dat het frequentiegebruik correct is geregistreerd bij het Agentschap Telecom.

4.3 Ontvangers van AIS-gegevens

Zoals in hoofdstuk 2 is beschreven, zendt het AIS-apparaat, kort gezegd, gegevens uit via radiogolven via een VHF-zender. De gegevens worden onversleuteld verzonden door het AIS-apparaat en kunnen in feite door iedereen met een juiste VHF-ontvanger worden ontvangen, mits deze op de juiste frequentie(s) is afgesteld en is uitgerust om de digitale AIS berichten te decoderen.

Artikel 9 van de RIS Richtlijn bepaalt dat lidstaten erop toe moeten zien dat de verwerking van persoonsgegevens, die gepaard gaat met het gebruik van RIS, plaatsvindt overeenkomstig de geldende wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. Lidstaten moeten daarom voorzien in veiligheidsmaatregelen en in hun toepassing om de RIS-berichten en -archieven te beschermen tegen ongewenste gebeurtenissen of tegen misbruik, met inbegrip van illegale toegang en wijziging of verlies van de gegevens.

In het besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart wordt herhaald dat de Wbp van toepassing is op de ontvangers van AIS-gegevens. In artikel 5 van dit besluit over het beheer en hergebruik van gegevens staat vermeld dat dit besluit alleen van toepassing is in de volgende situaties:[45]

- Wanneer een bevoegde autoriteit de gegevens heeft ontvangen op grond van een aankomst- of vertrekmelding overeenkomstig een van de toepasselijke wetten en de gegevens hij heeft ontvangen van een aan boord van een schip aanwezig AIS;

[43] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/adv/z2011-01003.pdf.
[44] Rapport EU 'Legal aspects of maritime monitoring & surveillance data', 2008 en Rapport ICR 'Protection of personal data when using Inland AIS devices', 2014.
[45] Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart, raadpleegbaar via: http://wetten.overheid.nl/BWBR0031560/2015-06-01.

- Wanneer een havenbeheerder de gegevens heeft verkregen op grond van de Wet voorkoming verontreiniging door schepen;
- Wanneer een bevoegde autoriteit de gegevens heeft ontvangen uit de te verschaffen inlichtingen als bedoeld in artikel 6 van de Verordening scheeps- en havenbeveiliging en artikel 3 van het Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart;
- Wanneer het aangewezen bestuursorgaan, bedoeld in artikel 4 (havenstaatcontrole) de gegevens heeft ontvangen ten behoeve van een uitgebreide inspectie; en
- Wanneer Onze Minister het heeft ontvangen in verband met de afgifte en het gebruik van het uniek Europees scheepsidentificatienummer.

De bovenstaande ontvangers betreffen allemaal bestuursorganen of publieke instanties. In deze wet- en regelgeving wordt aldus niet voorzien in de ontvangst van de gegevens door andere partijen. De Nederlandse wetgever heeft geen overige maatregelen getroffen ten aanzien van het gebruik van AIS-gegevens.

De Wbp is daarom onverkort van toepassing op de ontvangst van persoonsgegevens via AIS. Dit betekent dat iedere organisatie die dergelijke persoonsgegevens ontvangt een zelfstandig doel hiervoor nodig heeft. Daarnaast moet voor iedere organisatie een wettelijke grondslag bestaan op grond waarvan de organisatie de gegevens mag ontvangen.

Daarnaast bepaalt artikel 441 van het Wetboek van Strafrecht dat het niet toegestaan is om met een radio-ontvangerapparaat signalen op te vangen die niet voor hem bedoeld zijn en deze signalen vervolgens door te geven.[46]

Hieronder worden de verschillende ontvangers kort nader behandeld, waarbij een onderscheid wordt gemaakt tussen de vaarwegbeheerders en overige organisaties.

4.3.1 Vaarwegbeheerders

Verschillende organisaties zijn aangewezen als bevoegde autoriteiten in het kader van de Scheepvaartverkeerswet en mogen dus AIS-gegevens verwerken op basis van de wet en het besluit.

Het beheer van de scheepvaartwegen is in Nederland belegd bij verschillende bestuursorganen. Dit zijn het Rijk (belegd bij Rijkswaterstaat), de provincie, de gemeente en/of een ander openbaar lichaam, waaronder bijvoorbeeld havenmeesters en waterschappen. [47] Onder het beheer van een scheepvaartweg wordt verstaan het waterstaatkundig beheer van een scheepvaartweg.[48]

[46] Art. 441 WvSr “Met hechtenis van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft hij die de inhoud of de strekking van hetgeen door middel van een onder zijn beheer staande of door hem gebruikt radio-ontvangapparaat is opgevangen en, naar hij redelijkerwijs moet vermoeden, niet voor hem of mede voor hem bestemd is, hetzij aan een ander meedeelt, indien hij redelijkerwijs moet vermoeden, dat dan openlijke bekendmaking van de inhoud of de strekking volgen zal en zodanige bekendmaking volgt, hetzij openlijk bekend maakt.”
[47] Art. 2 lid 1 sub a Scheepvaartverkeerswet.
[48] Art. 1 lid 4 Scheepvaartverkeerswet.

Rijkswaterstaat

RWS is verantwoordelijk voor het vaarwegbeheer op rijkswateren.[49] Deze plicht kan worden afgeleid uit artikel 40 van de Binnenvaartwet en artikel 10.2 Binnenvaartregeling. Ten behoeve van het beheren van de vaarwegen heeft RWS daarom walinfrastructuur aangelegd om AIS-gegevens te ontvangen van de schepen die over deze vaarwegen varen. Deze gegevens worden door de RWS als vaarwegbeheerder gebruikt om te zorgen dat het verkeer over deze vaarwegen veilig en zo efficiënt mogelijk over de vaarwegen kan worden geleid.

Rijkswaterstaat verzamelt de gegevens voor een bepaald deel van het vaartraject en bewaart ze gedurende 18 minuten in het operationele systeem. Na 18 minuten zijn de gegevens niet meer nodig voor het directe managen van dat deel van de vaarweg. Op basis van de beschikbare informatie lijkt het erop dat de gegevens niet ook daadwerkelijk verwijderd worden uit het operationele systeem. Wel worden de gegevens elders opgeslagen voor historisch beheer (HAGO).

De technische infrastructuur die voor het operationeel management wordt gebruikt, wordt beheerd door RWS CIV (zie de hieronder). Op basis de beschikbare informatie lijkt het erop dat dit onderdeel van RWS zelf ook de gegevens verzamelt en bewaart.

RWS CIV

De RWS Centrale Informatievoorziening (RWS CIV) is een van de zes organisatieonderdelen van Rijkswaterstaat.[50] RWS CIV heeft blijkens artikel 3 lid 4 van het Besluit instellingen organisatieonderdelen Rijkswaterstaat 2013 vier taken:

- Het leveren en ontwikkelen van diensten op het gebied van informatievoorziening betreffende gegevens, applicaties en technische infrastructuur;
- Het leveren van expertise, leveren en ontwikkelen van kaders voor industriële automatisering in aanleg- en onderhoudscontracten;
- Het leveren van expertise en kennis op het gebied van informatievoorziening inclusief architectuur, en
- Het bijdragen aan de ontwikkeling en borging van kennis op het gebied van informatievoorziening.

RWS CIV heeft dus onder meer tot taak om infrastructuren aan te bieden en in stand te houden, onder andere die infrastructuren via welke de AIS-gegevens worden ontvangen, verder gezonden en opgeslagen. De vraag rijst echter of RWS CIV in haar hoedanigheid toegang moet hebben tot alle AIS-gegevens en deze gegevens mag opslaan of voor andere doeleinden mag gebruiken.

---

[49] https://www.rijkswaterstaat.nl/wegen/wetten-regels-en-vergunningen/wetten-aanleg-en-beheer/wet-beheer-rijkswaterstaatswerken.aspx.

[50] Art. 1 lid 2 sub b Besluit van de directeur-generaal van Rijkswaterstaat van 11 maart 2013, met kenmerk RWS/SDG-2013/12889, tot instelling van regionale en centrale organisatieonderdelen, programmadirecties en projectdirecties (Besluit instelling organisatieonderdelen Rijkswaterstaat 2013), raadpleegbaar via: https://zoek.officielebekendmakingen.nl/stcrt-2013-7577.html.

Het lijkt vanuit technisch oogpunt aannemelijk dat RWS CIV de gegevens opslaat gedurende de 18 minuten tijdens welke de gegevens voor het operationeel beheer gebruikt worden. Voor het operationeel beheer lijkt het niet noodzakelijk langere bewaartermijnen te hanteren. De rol van RWS CIV is echter onduidelijk ten aanzien van het historisch beheer (HAGO). Mocht in het kader van historisch beheer wel een rol zijn weggelegd voor RWS CIV, dan zouden voor dit doel aparte, wellicht langere, bewaartermijnen kunnen worden geïmplementeerd.

Havenmeesters

In navolging van artikel 40 van de Binnenvaartwet juncto artikel 10.2 van de Binnenvaartregeling worden de divisie Havenmeesters van Havenbedrijven Amsterdam N.V. en Rotterdam N.V. ook benoemd als bevoegde autoriteiten in het kader van de wet. Dit betekent dat zij op basis van dezelfde grondslag als RWS AIS-gegevens mogen verwerken voor het managen van hun deel van het Nederlandse vaarwegsysteem.

De havenmeester is in dienst bij de overheid en is belast met het toezicht op het veilig en economisch gebruik van een haven. Bovendien is het mogelijk dat de havenmeester toezicht houdt op de vaarwegen die tot de haven leiden. Havenmeesters worden door de gemeente aangewezen[51] en vallen daarmee onder artikel 2 lid 1 sub a onder 3 van de Scheepvaartverkeerswet. De havenmeester in Rotterdam is daarentegen werkzaam bij het havenbedrijf Rotterdam.[52]

Vanwege de vermenging van het publieke karakter met de commerciële kant van het Havenbedrijf, is het onduidelijk wie de AIS-gegevens verwerkt. Wel wordt duidelijk bij wet bepaald welke publiekrechtelijke taken de havenmeester moet uitvoeren.

Kustwacht

De Kustwacht is de vaarwegbeheerder voor de kustlijn van Nederland.[53] Blijkens het Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart mag de Kustwacht AIS-gegevens van schepen ontvangen.[54]

---

[51] http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/historie/Hoogheemraadschap%20Amstel,%20Gooi%20en%20Vecht/271860/271860_1.html, onder par. 2.2.

[52] Artikel 1 Besluit mandaat en machtiging havenmeester Rotterdam, beschikbaar via: http://wetten.overheid.nl/BWBR0027607/2012-03-24.

[53] https://www.rijkswaterstaat.nl/zakelijk/verkeersmanagement/scheepvaart/scheepvaartverkeersbegeleiding/river-information-services/automatic-identification-system/inland-ais-walinfrastructuur.aspx.

[54] Art. 15 Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart “Het Kustwachtcentrum stelt de gegevens die hij via AIS van een schip ontvangt ter beschikking aan kustwachtstations van andere lidstaten van de Europese Unie en aan de Europese Commissie en kan deze gegevens ook beschikbaar stellen aan een bevoegde instantie van een derde land. Indien het betreffende derde land geen partij is bij de overeenkomst betreffende de Europese Economische Ruimte is dit alleen mogelijk voor zover ten minste een gelijkwaardige bescherming van gegevens is gewaarborgd en nadat dit in een bestuursrechtelijke overeenkomst ter uitvoering van de doelstelling genoemd in artikel 1 van de richtlijn monitoring- en informatiesysteem zeescheepvaart is vastgelegd.” Deze informatie mag gedeeld worden met andere kuststations.

Omdat de Kustwacht niet vaarwegbeheerder is voor de binnenwateren, zal deze in het rapport alleen aan de orde komen ten aanzien van de plannen over het plaatsen van een gezamenlijke infrastructuur (zie hoofdstuk 7).

Overige vaarwegbeheerders

In navolging van artikel 40 van de Binnenvaartwet juncto artikel 10.3 van de Binnenvaartregeling zijn ook provincies, gemeentes en andere openbare instanties verantwoordelijk voor bepaalde vaarwegen.

Omdat dit buiten de scope van DGB van het ministerie I&M en RWS valt en omdat er geen informatie beschikbaar is gesteld over de verwerkingen door deze partijen, worden zij buiten beschouwing gelaten.

4.3.2 Doelen en grondslagen voor de gegevensverwerking door de vaarwegbeheerders

De vaarwegbeheerders hebben allerlei bevoegdheden en taken. Zij mogen deze taken enkel uitvoeren in het belang van onder meer het verzekeren van de veiligheid en het vlotte verloop van het scheepvaartverkeer.[55]

Op grond van artikel 4 lid 1 sub e Scheepvaartverkeerswet is het mogelijk om gegevens met betrekking tot de scheepvaart te ontvangen, bewaren en verstrekken door organisaties en personen die niet deelnemen aan het scheepvaartverkeer.[56]

Blijkens artikel 4 lid 3 Scheepvaartverkeerswet kunnen ten behoeve van een goede uitvoering van de River Information Services (RIS), en daarmee van AIS, persoonsgegevens worden verwerkt. De bevoegde autoriteit is verantwoordelijke voor deze verwerking.[57]

Dit betekent dat vaarwegbeheerders de AIS-gegevens, die als persoonsgegevens kunnen worden bestempeld, mogen ontvangen omdat deze noodzakelijk zijn voor de goede vervulling van de hierboven genoemde publiekrechtelijke taak (artikel 8 sub e Wbp).

4.4 Overige organisaties

Uit de gesprekken en uit onderzoek is gebleken dat er indicaties bestaan dat ook andere partijen, waaronder particulieren of private organisaties, de AIS-gegevens op enige wijze ontvangen. Dit blijkt onder andere uit het bestaan van websites en apps waarop de locaties en bewegingen van binnenvaartschepen gevolgd kunnen worden.[58] Daarbij moet worden

[55] Art. 3 lid 1 sub a Scheepvaartverkeerswet.
[56] Art. 4 lid 1 sub e Scheepvaartverkeerswet: Bij AMvB worden regels opgesteld met betrekking tot het ontvangen, bewaren en verstrekken van gegevens met betrekking tot de scheepvaart door organisaties en personen die niet deelnemen aan het scheepvaartverkeer.
[57] Art. 4 lid 4 Scheepvaartverkeerswet: Ter uitvoering van het eerste lid, onderdeel e, kunnen ten behoeve van de River Information Services persoonsgegevens worden verwerkt. De verwerking van deze gegevens vindt plaats teneinde een goede uitvoering te kunnen geven aan de bij of krachtens deze wet gestelde voorschriften omtrent de toepassing van River Information Services. De bij of krachtens algemene maatregel van bestuur aangewezen bevoegde autoriteit is verantwoordelijke voor deze verwerking.
[58] Een voorbeeld hiervan is de website MarineTraffic.com, VesselFinder.com en MyShipTracking en ShipFinder.com. Sommige websites, en andere aanbieders, bieden apps aan waarbij de locatie van schepen door middel van een AIS gevolgd kan worden.

opgemerkt dat het gedurende dit onderzoek niet duidelijk geworden is op welke wijze, dan wel via welke partijen, de genoemde organisaties de AIS-gegevens ontvangen.

4.4.1 Doelen en grondslagen voor de gegevensverwerking door overige organisaties

Ook de overige organisaties die de AIS-gegevens, waaronder persoonsgegevens, ontvangen, moeten een doel en een grondslag hebben om deze gegevens te mogen verwerken.

Enkel bestuursorganen kunnen eventueel een beroep doen op de verwerkingsgrondslag die gevonden wordt in artikel 8 sub e Wbp, de publiekrechtelijke taak. Daarom zal iedere private organisatie aansluiting moeten zoeken bij een andere grondslag in de Wet bescherming persoonsgegevens.

Een van deze grondslagen zou de toestemming van de schipper kunnen zijn. Het is mogelijk dat de schipper toestemming geeft aan websites of aan particulieren met een VHF-ontvanger om AIS-gegevens, en daarmee de bewegingen, van zijn of haar schip te ontvangen. Daarbij is het van belang dat deze toestemming geïnformeerd is en vrij en specifiek wordt gegeven. De schipper moet op basis van voldoende en duidelijke informatie deze keuze kunnen maken. Het moet de schipper daarnaast vrij staan om toestemming te weigeren. Bovendien moet hij zijn of haar toestemming altijd kunnen intrekken. Ten slotte moet het duidelijk zijn waarvoor de schipper precies toestemming geeft.

Tijdens de gehouden interviews en uit het onderzoek bleek dat het afhangt van de dienstverlening of de schipper toestemming geeft voor de verwerking van zijn of haar gegevens door bijvoorbeeld aanbieders van websites of particulieren. In Rotterdam is bijvoorbeeld een dienst aangeboden aan schippers om hen te waarschuwen wanneer uit AIS-gegevens blijkt dat de schipper te hard vaart.

Een ontvangende partij kan ook een gerechtvaardigd belang hebben om de AIS-gegevens te ontvangen (artikel 8 sub f Wbp). Dit is bijvoorbeeld het geval als schepen over en weer signalen ontvangen ten behoeve van het veilig varen. Maar naast deze grondslag, die direct voortvloeit uit het gebruik van AIS, kunnen er ook andere gerechtvaardigde belangen zijn. Daarbij moet de ontvangende organisatie afwegen of de gegevens daadwerkelijk noodzakelijk zijn voor het gerechtvaardigd belang dat de organisatie nastreeft. Daarbij zal iedere keer het belang van de organisatie om de gegevens te ontvangen, moeten worden afgewogen tegen de rechten en vrijheden van de schipper, met name diens recht op bescherming van de persoonlijke levenssfeer.

Ten slotte kunnen AIS-gegevens door organisaties verwerkt worden op grond van een wettelijke plicht. Dit betekent dat er op een organisatie een wettelijke plicht rust om persoonsgegevens te verwerken (artikel 8 sub c Wbp). Uit het onderzoek is vooralsnog van geen wettelijke plicht gebleken op basis waarvan de aanbieders van websites en particulieren de AIS-gegevens van de schipper zouden mogen verwerken.

5. Verdere verwerking van AIS-gegevens door vaarwegbeheerders

Naast het direct ontvangen van persoonsgegevens als onderdeel van de AIS-gegevens, is de Wbp ook van toepassing op alle handelingen die er vervolgens mee gedaan worden. Dit zijn immers ook verwerkingen. Ook aan deze verdere verwerkingen van persoonsgegevens kunnen risico's kleven. In dit hoofdstuk wordt nader aandacht besteed aan het verder verwerken van de persoonsgegevens door vaarwegbeheerders.

5.1 Zeggenschap over AIS-gegevens

Voordat wordt ingegaan op de verdere verwerkingen door de verschillende partijen die persoonsgegevens hebben verzameld doordat zij AIS-gegevens ontvangen, wordt hier eerst aandacht besteed aan het concept 'zeggenschap' of 'eigenaarschap' van persoonsgegevens.

Het is voor de verschillende betrokken partijen namelijk niet altijd duidelijk hoe met persoonsgegevens omgegaan moet worden en op basis van welke grondslag gegevens kunnen worden verwerkt. Mede hierdoor verwerken organisaties AIS-gegevens omdat ze menen 'eigenaar' te zijn van de gegevens of omdat ze menen 'zeggenschap' over de gegevens te hebben.

Onder de Wbp is het echter niet mogelijk om ‘eigenaar’ van gegevens te zijn. Eigenaar is men namelijk enkel van goederen (zaken en vermogensrechten). Een persoonsgegeven is geen goed, men kan hier dus geen eigenaar van zijn. Ook het individu zelf kan niet altijd bepalen wie toegang heeft tot bepaalde gegevens over hem of haar. Zo kan men bijvoorbeeld de Belastingdienst niet weigeren bepaalde gegevens te verwerken.

Zoals in hoofdstuk 2 is aangegeven, gaat het er om of de organisatie in kwestie een legitiem doel heeft en of er een rechtsgrondslag is om de gegevens te mogen verwerken. Dit betekent dat mogelijk meerdere organisaties de gegevens kunnen verwerken. Een situatie hiervan is bijvoorbeeld de schipper die de AIS-gegevens aan het havenbedrijf ter beschikking stelt zodat dit bedrijf een ligplaats voor hem kan reserveren. Ook is het mogelijk dat de schipper de AIS-gegevens ter beschikking stelt aan een organisatie zodat een vaarplanning kan worden opgesteld. Dit betekent evenwel niet dat de schipper hiermee per definitie altijd bepaalt waar de gegevens voor mogen worden verwerkt. Zoals eerder genoemd, hebben de vaarwegbeheerders in het kader van hun publiekrechtelijke raak ook de mogelijkheid om de AIS-gegevens te verzamelen, met of zonder toestemming van de schipper.

Wanneer toestemming als grondslag wordt gebruikt, moet het individu deze wel ondubbelzinnig gegeven hebben.

Verantwoordelijkheid

Zoals hierboven is aangegeven, zijn er mogelijk meerdere partijen die persoonsgegevens mogen verwerken, maar dit betekent evenwel niet dat deze partijen vervolgens zelf mogen bepalen waarvoor de gegevens verder worden verwerkt. Voor het verder verwerken van

gegevens is de Wbp nog steeds leidend en moet bepaald worden op basis van welke grondslag de persoonsgegevens voor andere doelen mogen worden gebruikt en eventueel beschikbaar mogen worden gesteld aan anderen. En of deze verdere verwerking verenigbaar is met het oorspronkelijke doel.

Om deze overwegingen te maken en de beslissingen te nemen, krijgt het aanbeveling om binnen de betreffende organisatie iemand aan te wijzen, die ervoor zorgt dat door de betreffende organisatie de persoonsgegevens conform de wet worden verwerkt en dat dit wordt vastgelegd.

Het beeld dat op basis van de beschikbare informatie is ontstaan, is dat verschillende personen en/of afdelingen binnen een vaarwegbeheerder, waaronder RWS, AIS-gegevens verwerken en hierover naar eigen inzicht beschikken, zonder dat duidelijk is op basis van welke grondslag en voor welke doelen dit gebeurt.

5.2 Primair doel AIS: verkeersmanagement door vaarwegbeheerders

Zoals in de voorgaande hoofdstukken is aangegeven, heeft de Nederlandse wetgever de RIS-Richtlijn in de Scheepvaartverkeerswet geïmplementeerd. In de Scheepvaartverkeerswet zijn de River Information Services gedefinieerd als de geharmoniseerde informatiediensten ter ondersteuning van het verkeers- en vervoersmanagement voor de binnenvaart, met inbegrip van de technisch haalbare koppelingen met andere vervoerswijzen dan wel met commerciële activiteiten, niet zijnde interne commerciële activiteiten tussen betrokken bedrijven.[59] Met andere woorden, het doel van de Nederlandse implementatie van AIS is verkeersmanagement.

Zoals de wetgever zelf al bij de implementatie van de RIS-Richtlijn heeft aangegeven, levert het gebruik van AIS op de binnenwateren een belangrijke bijdrage aan zowel de veiligheid als de doeltreffendheid van het vervoer over deze wateren. De invoering van AIS heeft onder meer tot doel de planning en het beheer van het verkeer en het vervoer op de binnenwateren te ondersteunen. Binnenschippers kunnen bijvoorbeeld sneller de juiste navigatiebeslissingen nemen. Ook is het makkelijker voor de binnenschippers om met behulp van AIS een planning voor de langere termijn op te stellen.[60]

Hoewel de invoering van AIS is bedoeld voor het verkeersmanagement is er veel discussie over de reikwijdte hiervan en wordt in sommige gevallen voorgestaan om ook vaarwegmanagement hieronder wordt verstaan De relatie tussen verkeersmanagement en vaarwegmanagement is hierdoor niet altijd duidelijk.

Verkeersmanagement zelf moet strikt worden geïnterpreteerd. AIS-gegevens mogen in feite enkel gebruikt worden om het vaarverkeer op locatie in goede banen te leiden, bijvoorbeeld voor inhaalmanoeuvres maar ook bij sluizen en voor de communicatie met de verkeerscentrales.

[59] Art. 1 lid 1 sub p Scheepvaartverkeerswet.
[60] Kamerstukken II, 2006-2007, 30974, nr. 3, p. 2.

Een ruimere interpretatie van verkeersmanagement laat gebruik van AIS bijvoorbeeld ook toe zodat verkeersposten schepen automatisch kunnen identificeren waardoor het niet meer nodig is dat schepen zich moeten melden.

Nog ruimere interpretaties bieden de mogelijkheid dat AIS-gegevens gebruikt kunnen worden voor *corridormanagement.* Hieronder kan onder meer worden begrepen het efficiënter verkeersmanagement en de verbetering van de dienstverlening door de vaarwegbeheerders, havens en ligplaatsbeheerders. Op basis van AIS-gegevens zouden schippers geadviseerd kunnen worden over de te varen route, de aan te houden snelheid, de planning van de reis etc. Hierdoor worden de reistijden betrouwbaarder. Bovendien kan er worden gehandeld wanneer blijkt dat het op een bepaald stuk water erg druk gaat worden. Ten behoeve hiervan moeten schepen continu worden gevolgd.

Daarnaast zien sommigen het maken van modellen als een vorm van verkeersmanagement. Op basis van deze modellen kan worden vastgesteld, en eventueel worden voorspeld, welke schepen (met welke lading) op weg zijn naar welke bestemming. Ook rijst de vraag of ligplaatsbeheer in bijvoorbeeld havens, de heffing van havengelden of capaciteitsmanagement onder verkeersmanagement valt.

Tenslotte is RWS bezig met de ontwikkeling van apps ten behoeve van de veiligheid van pleziervaart. Aan de hand van deze apps kan de pleziervaart zien welke binnenschepen langs zullen varen. Omdat RWS hiermee AIS-gegevens, waaronder persoonsgegevens, beschikbaar stelt aan het publiek, zal moeten worden bepaald op basis van welke rechtsgrondslag het deze persoonsgegevens kan verstrekken aan derde partijen en dus of de verstrekking valt binnen de publiekrechtelijke taak van vaarwegmanagement.

Verenigbaar of onverenigbaar doel

Omdat er onduidelijkheid is over wat er nog onder de publiekrechtelijke taak van verkeersmanagement valt, bestaat er ook onduidelijkheid over de vraag of het bovenstaande gebruik van de AIS-gegevens nieuwe doelen betreft of dat het nog onder hetzelfde doel valt.

Het gevolg hiervan is dat het niet altijd duidelijk is op basis van welke grondslag de gegevens verwerkt worden en of dit wel is toegestaan. In hoofdstuk 2 is namelijk toegelicht dat gegevens alleen voor het specifieke doel gebruikt mogen worden of voor een verenigbaar doel. Als er onduidelijkheid is over het specifieke doel, is het dus ook onduidelijk of de verwerkingen allemaal nog binnen dit doel passen of dat er sprake is van een ander doel.

Dan is de vervolgvraag of dit andere doel verenigbaar is of niet. Indien het verenigbaar is, mogen de gegevens in principe voor dit nieuwe doel worden verder verwerkt, mits er ook voor dit nieuwe doel een rechtsgrondslag bestaat. Dit zal per geval bepaald moeten worden.

In de aankomende Algemene verordening gegevensbescherming zal het niet meer nodig zijn om een nieuwe grondslag voor de verdere verenigbare verwerking te hebben. Niettemin moet wel worden bepaald of het doel verenigbaar is.

De Europese wetgever heeft in de Avg enkele indicatoren opgenomen aan de hand waarvan bepaald moet worden of een gegeven verder verwerkt wordt voor een verenigbaar doel als waarvoor de gegevens aanvankelijk zijn verzameld. De verantwoordelijke zal onder meer rekening moeten houden met:

- Het verband tussen het doel waarvoor de AIS-gegevens in eerste instantie verzameld zijn;
- Het doel waarvoor de verantwoordelijke de AIS-gegevens nu wil verwerken;
- Het kader waarin de AIS-persoonsgegevens zijn verzameld. Hierbij weegt met name de verhouding tussen de schipper en de verantwoordelijke mee;
- De aard van het AIS-persoonsgegeven. Hierbij speelt de vraag mee of bijzondere persoonsgegevens worden verwerkt. Zoals aangegeven maken locatiegegevens onderdeel uit van AIS-gegevens. Deze gegevens worden door de Autoriteit Persoonsgegevens als gevoelige persoonsgegevens bestempeld;
- De mogelijke gevolgen van de voorgenomen verwerking voor de schipper moeten worden meegewogen. Daarbij speelt mee dat de vermoedelijk locatie van de schipper, diens familie en diens woning continu wordt gevolgd;
- Of er passende waarborgen bestaan, bijvoorbeeld of er sprake is van versleuteling of pseudonimisering van de AIS-gegevens.[61]

Wanneer vastgesteld wordt dat de verdere verwerking van AIS-gegevens niet geschiedt op basis van een verenigbaar doel, dan mogen de gegevens niet verder worden verwerkt.

5.3 Gebruik AIS-gegevens voor verkeersmanagement

Binnen RWS worden de AIS-gegevens onder meer gebruikt voor het beheer van de vaarwegen. Deze vaarwegen worden onder andere gebruikt voor de scheepvaart. Bij het beheer van deze vaarwegen wordt onderscheid gemaakt naar vaarwegbeheer en nautisch beheer:

- Vaarwegbeheer is het in stand houden van de scheepvaartweg ten behoeve van de scheepvaart door baggeren, het vrijhouden van obstakels en onderhoud van oevers en kunstwerken, waaronder sluizen.
- Het nautisch beheer, en de Scheepvaartverkeerswet, beoogt de regeling van het scheepvaartverkeer met het oog op het vlotte verloop, de veiligheid van het scheepvaartverkeer en het voorkomen van risico's en schade door de scheepvaart.[62] Het nautisch beheer kan wederom worden onderverdeeld in:
    - Operationeel beheer;
    - Historisch beheer.

[61] Art. 6 lid 4 sub a tot en met e en Overweging 50 Avg.
[62] http://www.watererfgoed.nl/links/19_toelicht_vaarvergunningen.pdf, p. 1.

Door middel van de systemen die worden gebruikt voor het operationeel beheer en het historisch beheer van AIS geeft RWS invulling aan haar interpretatie van vaarwegmanagement.

Nautisch beheer is geregeld in Besluit Administratieve Bepalingen Scheepvaartverkeer en in het Binnenvaartpolitiereglement.[63]

Operationeel beheer

Het AIS-apparaat van een schip zendt allerlei ruwe en privacygevoelige gegevens uit. Deze gegevens worden opgevangen door alle andere schepen uitgerust met een AIS-apparaat en door de AIS-walinfrastructuur.[64] Alle walinfrastructuren leveren de ontvangen AIS-gegevens die in een operationeel systeem samen komen. Dit gebeurt op basis van een convenant, dat inmiddels is verlopen. Door deze gegevens samen te voegen, ontstaat een beeld over de verkeerssituatie.

Op basis van de beschikbare informatie is gebleken dat er een RWS-website is met besloten toegang, waarop deze verkeerssituatie kan worden ingezien voor het beheer van sluizen en bruggen. Deze website is beveiligd met een gebruikersnaam en een wachtwoord en zij is daarmee niet publiek toegankelijk.

Het gebruiken en verzamelen van AIS-gegevens voor operationeel beheer is noodzakelijk zolang de gegevens van een schip bruikbaar zijn voor identificatie en veiligheid. Over het algemeen bedraagt deze tijd 18 minuten. De gegevens moeten voor het doel van operationeel beheer verwijderd worden zodra de gegevens niet langer noodzakelijk zijn voor het operationeel beheer.

Om te bepalen of de AIS-gegevens voor operationeel beheer gebruikt kunnen worden, zal moeten worden bepaald of deze gegevens worden verwerkt voor of in overeenstemming met het oorspronkelijke doel vaarwegmanagement.

Ook moet worden gekeken naar het kader waarin de AIS-gegevens zijn verzameld. Hierbij weegt met name de verhouding tussen de schipper en de vaarwegbeheerder mee. De schipper heeft de wettelijke plicht om de AIS-gegevens uit te zenden. De vaarwegbeheerder heeft op haar beurt de taak om het beheer van de vaarwateren en het management van de vaarwateren te borgen.

Daarnaast moet de aard van het AIS-persoonsgegeven worden meegewogen bij de vraag of het gegeven voor een verenigbaar doel verder wordt verwerkt. Hierbij speelt de vraag mee of bijzondere persoonsgegevens worden verwerkt. Zoals aangegeven, maken locatiegegevens onderdeel uit van AIS-gegevens. Deze gegevens worden door de Autoriteit Persoonsgegevens als gevoelige persoonsgegevens gekwalificeerd.

---

[63] http://www.watererfgoed.nl/links/19_toelicht_vaarvergunningen.pdf.

[64] https://www.rijkswaterstaat.nl/zakelijk/verkeersmanagement/scheepvaart/scheepvaartverkeersbegeleiding/river-information-services/automatic-identification-system/inland-ais-walinfrastructuur.aspx.

Bovendien moet de verantwoordelijke de mogelijke gevolgen van de voorgenomen verwerking voor de schipper meewegen. Daarbij speelt mee dat de vermoedelijk locatie van de schipper, diens familie en diens woning continu wordt gevolgd.

Ten slotte speelt een rol of er passende waarborgen bestaan, bijvoorbeeld of er sprake is van versleuteling of pseudonimisering van de AIS-gegevens.[65] Hierbij weegt mee dat de gegevens die worden verwerkt voor operationeel beheer, verwerkt worden om deze beschikbaar te stellen op een website. Deze website is niet algemeen toegankelijk en kan enkel worden geraadpleegd voor het beheer van sluizen en bruggen.

De vaarwegbeheerder zal moeten bepalen of de gegevens die voor operationeel beheer worden verwerkt binnen de definitie van vaarwegbeheer vallen of, aan het hand van deze voorgenoemde criteria, moeten argumenteren of deze gegevens worden verwerkt voor een ander doel.

Om risico's te voorkomen, zal onder meer moeten worden nagedacht over de vraag hoe lang de gegevens die in dit operationele systeem staan, bewaard worden. Gegevens mogen immers zo lang worden bewaard als ze noodzakelijk zijn. Na verloop van tijd zal het niet meer noodzakelijk zijn om de gegevens te hebben. Dan zullen de gegevens moeten worden verwijderd.

Historisch beheer

De gegevens uit het hiervoor genoemde operationele systeem worden maandelijks geëxporteerd naar het systeem waar gegevens voor historisch beheer worden opgeslagen (HAGO). Deze gegevens stammen van de Kustwacht, AIS Walinfra/DIAMONIS, de Schelde Radar Keten, de Haven van Rotterdam en Satelliet AIS.[66] Mogelijk wordt dit in de toekomst uitgebreid met informatie van de Nederlandse provinciën. Op basis van de gegevens worden bijvoorbeeld analyses gemaakt, statistieken opgesteld en beleid ontwikkeld en geëvalueerd.

Het is van groot belang dat bepaald wordt voor welke doelen, en op basis van welke grondslag, de AIS-gegevens in HAGO worden opgeslagen en vervolgens worden gebruikt.

Wanneer de AIS-gegevens worden opgeslagen in HAGO is er sprake van een verdere verwerking. Daarbij zal men moeten nagaan of de AIS-gegevens uit HAGO worden gebruikt ter uitvoering van verkeersmanagement of ter uitvoering van een ander doel. Vervolgens moet worden bepaald of dit andere doel verenigbaar is en of hiervoor een rechtsgrondslag is.

De Wbp voorziet erin dat het verder verwerken van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden als een verenigbaar doel met verkeersmanagement moet worden beschouwd. Het is dan wel van belang dat RWS de

[65] Art. 6 lid 4 sub a tot en met e en Overweging 50 Avg.
[66] Bron 20160307 AIS-HAGO Tekening Gegevensstromen.

nodige voorzieningen heeft getroffen zodat wordt gewaarborgd dat de AIS-gegevens alleen voor deze doeleinden worden gebruikt.[67]

Als men de AIS-gegevens in HAGO voor andere doelen wil verwerken, of deze verenigbaar zijn en zal moeten worden nagegaan op basis van welke rechtsgrondslag dit gebeurt. Wanneer wordt vastgesteld dat RWS een grondslag heeft om de AIS-gegevens in HAGO op te slaan en vervolgens te gebruiken, is het van belang dat nagedacht wordt over de vraag op welke wijze de gegevens in HAGO worden opgeslagen.

Met de principes van dataminimalisatie en '*privacy by design & by default*' in gedachte moet ook worden bepaald of de AIS-gegevens als zodanig opgeslagen moeten worden, of dat de gegevens geanonimiseerd kunnen worden verwerkt. Voor bepaalde doeleinden is het namelijk wellicht ook mogelijk om de gegevens op geanonimiseerde wijze beschikbaar te stellen. Denk hierbij aan meer statistische informatie over het aantal schepen dat een bepaalde sluis heeft gepasseerd en de lengte van deze schepen.

De Wbp en straks ook de Avg, schrijven namelijk voor dat niet meer gegevens mogen worden verwerkt dan noodzakelijk voor het doel. Hierbij moet ook aandacht worden besteed aan de proportionaliteit en de subsidiariteit van de verwerking.

Tenslotte is het ook in dit geval van belang om te bepalen hoe lang de gegevens bewaard dienen te worden. Na verloop van tijd zal het niet meer noodzakelijk zijn om de gegevens te hebben. Dan zullen de gegevens moeten worden verwijderd.

5.4 Verstrekken van AIS-gegevens aan publieke partijen

Zoals uit de bovenstaande paragrafen blijkt, worden door RWS als vaarwegbeheerder via de walinfrastructuur AIS-gegevens, waaronder persoonsgegevens, verwerkt. De partij die wordt gebruikt voor de technische ondersteuning, is RWS CIV en de gegevens worden zowel voor operationeel beheer als voor historisch beheer ergens opgeslagen. Op basis van de verkregen informatie lijken op meerdere plaatsen binnen RWS AIS-gegevens te worden verwerkt.

Los van de vraag of al deze instanties de gegevens in overeenstemming met de wet verwerken, hebben de instanties in potentie de mogelijkheid dat zij de gegevens verder verstrekken aan andere partijen.

Hieronder volgen de mogelijke partijen aan wie de vaarwegbeheerder, met de grootste nadruk op RWS, de gegevens verstrekt.

Aan andere vaarwegbeheerders

De verschillende vaarwegbeheerders zouden op allerlei manieren AIS-gegevens met elkaar kunnen delen. De vraag is echter of dit wettelijk gezien is toegestaan. Zoals hierboven uiteengezet, mogen vaarwegbeheerders op grond van hun publiekrechtelijke taak AIS-gegevens ontvangen en verwerken. Vaarwegbeheerders zullen echter altijd moeten toetsen

[67] Art. 9 lid 3 Wbp.

of het voor de uitoefening van hun specifieke publiekrechtelijke taak noodzakelijk is dat zij bepaalde AIS-gegevens ontvangen.

Hierbij is ook van belang om te bepalen voor welk deel van het Nederlandse vaarwegennet de vaarwegbeheerder bij wet is aangewezen als de vaarwegbeheerder. Alleen de gegevens die noodzakelijk zijn voor het beheer van dat deel van de wateren waar de organisatie bevoegd is, zullen noodzakelijk zijn voor het uitoefenen van de publiekrechtelijke taak.

Wanneer een schip richting een haven koerst, is het dus wellicht binnen zijn taak dat de havenmeester bepaalde AIS-gegevens moet ontvangen. Dit kan anders liggen wanneer een schip de haven vanaf Maastricht richting de haven van Rotterdam vaart, maar een havenbeheerder in bijvoorbeeld Groningen de AIS-gegevens zou willen ontvangen.

Eenzelfde afweging moet worden gedaan ten aanzien van een gezamenlijk systeem voor bijvoorbeeld het IJsselmeer: de verstrekkende vaarwegbeheerder zal zich moeten afvragen of hij een grondslag heeft om deze gegevens te verstrekken. De overige vaarwegbeheerders zullen moeten nagaan of zij een grondslag hebben om de gegevens te ontvangen.

Een vaarwegbeheerder zal zich dus altijd moeten afvragen of de AIS-gegevens die hij wenst te ontvangen of wenst te verstrekken noodzakelijk zijn voor de uitoefening van zijn publiekrechtelijke taak of dat er een andere rechtsgrondslag, als opgesomd in hoofdstuk 2, van toepassing is.

Het is goed om op te merken dat in sommige gevallen de havenmeester in dienst is bij het (particuliere) havenbedrijf. Bovendien komt het voor dat het particuliere havenbedrijf de AIS-gegevens voor de havenmeester bewerkt. De havenmeester is dan verantwoordelijke in de zin van de Wbp en het havenbedrijf is bewerker ten behoeve van de havenmeester. Het is daarbij van belang dat het havenbedrijf deze gegevens niet voor andere doeleinden gaat gebruiken, en daarmee zelf verantwoordelijke voor de gegevens wordt, maar dat het havenbedrijf zich aan de aanwijzingen van de havenmeester houdt.

Politie en justitie t.b.v. opsporing ('vordering')

In verband met de opsporing kunnen politie en justitie de AIS-gegevens vorderen van ontvangers van AIS-gegevens. Dit blijkt uit artikel 9 lid 1 sub c Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart. Volgens dit artikel moet een ontvanger van AIS-gegevens deze gegevens verstrekken aan ambtenaren die op grond van artikel 141 Wetboek van Strafrecht belast zijn met de opsporing van strafbare feiten, in navolging van de artikelen 126nc en 126nd Wetboek van Strafvordering. Er moet wel gericht naar deze gegevens gevraagd zijn.

Bovendien moet de ontvanger van de AIS-gegevens blijkens sub d van hetzelfde artikel de ambtenaren van de politie die zijn aangesteld voor de uitvoering van de politietaak verstrekken, wederom voor zover er gericht naar deze gegevens is gevraagd.[68]

[68] Art. 9 lid 1 Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart: "Een ontvanger van gegevens, bedoeld in artikel 5, geeft, buiten de in artikel 8 bedoelde gevallen, slechts na een daartoe strekkend verzoek inzage in door hem ontvangen gegevens of verstrekt deze gegevens aan:

Toezicht en handhaving

Zoals in eerdere paragrafen is uitgewerkt, zal moeten worden bepaald of handhaving door publieke organisaties zoals RWS, de Inspectie Leefomgeving en Transport (ILT), de lokale vaarwegbeheerders en de politie binnen het oorspronkelijke doel waarvoor de AIS-gegevens zijn verzameld valt, namelijk verkeersmanagement. Wanneer dit niet het geval is, zal moeten worden bepaald of er sprake is van een verenigbaar doel is en zo ja, op basis van welke grondslag de verwerking mag geschieden.

In het eerder genoemde en verlopen convenant met betrekking tot de levering van AIS-gegevens door de walinfrastructuren aan het operationeel systeem was bepaald dat AIS-gegevens niet ook voor handhavingsdoeleinden mogen worden gebruikt. Op dit moment lijken alle partijen ook te beamen dat de gegevens hier (nog) niet voor worden gebruikt, maar omdat het convenant verlopen is en geen nieuw convenant bestaat, is het de vraag hoe lang dit nog de situatie zal zijn.

Mocht het gebeuren dat AIS-gegevens ook voor toezicht- en handhavingsdoeleinden gebruikt mogen worden, is het wel zaak dat helder uit de grondslag blijkt dat dit inderdaad mag, bijvoorbeeld door een aanpassing van de wetgeving.

5.5 Verstrekken van AIS-gegevens aan private partijen

Er zijn allerlei aanwijzingen dat verschillende private partijen toegang hebben tot de AIS-gegevens en deze voor allerlei doeleinden verwerken. Hieronder wordt een overzicht gegeven.

Voordat wordt in gegaan op de verschillende partijen is het van belang te benadrukken dat een schipper verplicht is AIS-gegevens uit te zenden en dat de gegevens onversleuteld worden verzonden. Dit betekent dat het systeem *an sich* niet privacy-vriendelijk is. Door de voortschrijding van de techniek zou door de wetgever kunnen worden overwogen of de verplichting om bepaalde gegevens door schippers te laten uitzenden ten behoeve van het vaarwegbeheer op een privacy-vriendelijker manier invulling kan worden geven.

Dit laat onverlet de verplichtingen op alle verantwoordelijken, ook die organisaties die geen vaarwegbeheerders zijn, om bij het verwerken van AIS-gegevens te voldoen aan de geldende wet- en regelgeving, waaronder de Wbp.

CBS, TNO & studenten

Het CBS en TNO doen (statistische) onderzoeken met de AIS-gegevens. Daarnaast komt het voor dat studenten voor onderzoeksdoeleinden de AIS-gegevens willen gebruiken.[69]

(..)
sub c: ambtenaren die bij of krachtens artikel 141 van het Wetboek van Strafvordering belast zijn met de opsporing van een strafbaar feit voor zover gericht naar gegevens wordt gevraagd;
sub d: ambtenaren van politie die zijn aangesteld voor de uitvoering van de politietaak voor zover gericht naar gegevens wordt gevraagd."

[69] Overweging 50 Avg: verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, moeten als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking worden beschouwd.

RWS mag de gegevens doorgeven aan deze partijen wanneer RWS hiervoor een grondslag heeft. RWS heeft de AIS-gegevens immers zelf verzameld ten behoeve van verkeersmanagement. Als de genoemde organisaties AIS-gegevens verder verwerken voor historische, statistische of wetenschappelijke doeleinden kan dit als een verenigbaar doel met verkeersmanagement worden beschouwd, mits voldoende waarborgen worden getroffen.[70] Het is dan wel van belang dat de verantwoordelijke de nodige voorzieningen heeft getroffen zodat wordt gewaarborgd dat de AIS-gegevens alleen voor deze doeleinden worden gebruikt.[71] In dat geval kan RWS de AIS-gegevens voor deze doeleinden doorgeven.

Als de organisaties de AIS-gegevens voor andere doelen dan historische, statistische of wetenschappelijke doelen wil gebruiken, zal moeten worden nagegaan of RWS op grond van een ander doel en een andere grondslag de gegevens aan deze partijen kan doorgeven.

Havenbedrijf

In de meeste havens is er naast de havenmeester ook een havenbedrijf. Dit havenbedrijf is meestal in particuliere handen. Havenbedrijven, zoals het Havenbedrijf Rotterdam, beheren, exploiteren en ontwikkelen de haven en het eventueel daarbij horende industriegebied. Het Havenbedrijf Rotterdam is onder meer verantwoordelijk voor het handhaven van een veilige en vlotte afhandeling van de scheepvaart.[72] Ten behoeve hiervan zijn AIS-gegevens nuttig. Deze kunnen bijvoorbeeld worden gebruikt voor het ligplaatsbeheer in een haven.

Om de AIS-gegevens voor dit doel te mogen ontvangen, heeft de versturende partij een wettelijke grondslag nodig. Het is mogelijk dat het havenbedrijf de toestemming van de schipper vraagt om diens gegevens voor bijvoorbeeld ligplaatsbeheer in de haven te gebruiken (artikel 8 sub a Wbp). Daarnaast zou de haven een gerechtvaardigd belang kunnen hebben om de AIS-gegevens voor ligplaatsbeheer te kunnen gebruiken (artikel 8 sub f Wbp). In dat geval kunnen de AIS-gegevens worden verstrekt als dat noodzakelijk is voor de behartiging van een gerechtvaardigd belang van het havenbedrijf. Daarbij moet worden afgewogen of de rechten van de schipper, in het bijzonder diens recht op bescherming van zijn persoonlijke levenssfeer, prevaleert.

Websites en apps

Tenslotte bestaan er allerlei websites waar in *real time* de bewegingen van een schip gevolgd kan worden.[73] Het is onduidelijk hoe deze websites aan de AIS-gegevens komen. Het is niet uitgesloten dat particulieren de VHF-ontvangers in huis hebben, de AIS-signalen van de voorbijvarende schepen opvangen en de informatie doorgeven aan deze websites.

Wanneer particulieren deze gegevens uitsluitend opvangen voor persoonlijke of huishoudelijke doeleinden, is de Wet bescherming persoonsgegevens niet van toepassing (artikel 2 lid 2 sub a Wbp) en kunnen particulieren vanuit privacy-perspectief deze gegevens ontvangen. Mocht het echter voorkomen dat private organisaties deze gegevens gebruiken,

[70] Artikel 9 lid 3 Wbp.
[71] Art. 9 lid 3 Wbp.
[72] https://www.portofrotterdam.com/nl/havenbedrijf/over-het-havenbedrijf.
[73] Een bekend voorbeeld is Marinetraffic.com.

zullen deze organisaties als verantwoordelijke in de zin van de wet worden gezien en moeten zij een doel en een grondslag hebben en zich houden aan de overige zorgvuldigheidsverplichtingen.

De beheerders van de betreffende websites en apps publiceren de gegevens op internet via onder andere *real time* kaarten. Naar het zich laat aanzien, is de enige grondslag die deze partijen kunnen aanvoeren voor het publiceren van deze gegevens die van het gerechtvaardigd belang (artikel 8 sub f Wbp). Nu het om (onder andere) locatiegegevens gaat, is het aannemelijk dat het Autoriteit Persoonsgegevens van oordeel is, dat het privacybelang van de schipper prevaleert boven het belang van dit soort websites en haar bezoekers om *real time* inzicht in binnenvaart bewegingen te hebben.

5.6 Relatie met de 'open data'-verplichting

Steeds meer overheidsinstanties publiceren de gegevens die zij bezitten in navolging van de Wet openbaarheid bestuur. Meer en meer databanken, die traditioneel alleen in handen zijn van de overheid, worden toegankelijk gemaakt voor het grote publiek. Het is belangrijk dat de overheid goed nadenkt over de privacy-implicaties voor individuen voordat het gegevens toegankelijk maakt. Dit geldt ook in het geval de gegevens geanonimiseerd zijn. Het kan namelijk zijn dat geanonimiseerde gegevens, in combinatie met andere gegevens, wel weer tot een schipper herleidbaar worden, waardoor het weer persoonsgegevens zijn.

Dit geldt uiteraard ook indien gegevens geanonimiseerd worden verstrekt aan derde partijen, bijvoorbeeld vanuit het historische beheer (HAGO). Ook dan moet er dus bepaald worden of de ontvangende organisatie de gegevens makkelijk herleidbaar kan maken tot een individu.

5.7 Verantwoordelijkheid bij aanbestedingen

Wanneer een publieke organisatie samenwerkt met derde partijen, niet in de rol van verantwoordelijke of bewerker, maar bijvoorbeeld in het kader van een aanbestedingsprocedure, rijst de vraag tot hoe ver de verantwoordelijkheid van de overheid gaat. Ook al rust er niet direct een verantwoordelijkheid in termen van de Wbp op de overheid, wanneer de andere partijen niet correct omgaan met de persoonsgegevens, kan dit wel degelijk een negatieve invloed hebben op de publieke organisatie in kwestie.

6. Verdere verwerking van AIS-gegevens door andere partijen dan vaarwegbeheerders

In het vorige hoofdstuk is ingegaan op het verder verwerken van AIS-gegevens door vaarwegbeheerders, maar zoals eerder in dit rapport aangegeven, kunnen AIS-gegevens ook door andere partijen worden ontvangen. Wanneer deze partijen de AIS-gegevens, waaronder dus persoonsgegevens, verder willen verstrekken, is de Wbp ook van toepassing op alle handelingen die vervolgens met de gegevens gedaan worden. Dit zijn immers ook verwerkingen. Ook aan deze verdere verwerkingen van persoonsgegevens kunnen risico's kleven.

Verschillende partijen verwerken de AIS-gegevens voor allerlei doeleinden, die niet allemaal bekend zijn op basis van de beschikbare informatie. Niettemin is het ook in deze gevallen van belang dat gegevens alleen verder mogen worden verwerkt als hiervoor een doel en een grondslag is vastgesteld.

Havenbedrijf

Daar waar de Havenmeester onderdeel is van het Havenbedrijf of hier zeer nauwe relaties mee heeft, bestaat het risico dat de ontvanger de AIS-gegevens niet alleen ter uitoefening van de publiekrechtelijke taak van vaarwegbeheer, maar de gegevens ook voor andere doeleinden worden gebruikt, bijvoorbeeld voor het innen van havengeld. Zoals gezegd, mag dit alleen maar als dit gebruik verenigbaar is met het doel van vaarwegbeheer en wanneer hier een aparte rechtsgrondslag voor bestaat.

Ter beantwoording van de vraag of het innen van havengelden een verenigbaar doel is, zijn een aantal indicatoren opgesteld door de EU-wetgever. Hiervoor wordt verwezen naar paragraaf 5.2 van dit rapport.

Wanneer een andere grondslag noodzakelijk is, zou bijvoorbeeld de schipper om toestemming kunnen worden gevraagd om de AIS-gegevens van zijn schip te gebruiken voor het innen van havengelden. Wanneer mogelijk, kan de havenmeester ook bepalen of de verwerking kan worden gebaseerd op zijn gerechtvaardigde belang om de AIS-gegevens te gebruiken om havengelden te innen (artikel 8 sub f Wbp). Hierbij moeten de rechten en vrijheden van de schipper worden afgewogen tegen het belang van de havenmeester om het havengeld te innen.

Politie en justitie t.b.v. opsporing ('vordering')

In verband met de opsporing kunnen politie en justitie de AIS-gegevens vorderen van ontvangers van AIS-gegevens. In navolging van de artikelen 126nc en 126nd Wetboek van Strafvordering [74] moet een organisatie die AIS-gegevens verwerkt deze gegevens verstrekken aan ambtenaren die op grond van artikel 141 Wetboek van Strafrecht belast zijn met de opsporing van strafbare feiten. Er moet wel gericht naar deze gegevens gevraagd zijn. Bovendien moet de ontvanger van de AIS-gegevens verstrekken aan de ambtenaren

[74] Afhankelijk van de kwalificatie als elektronische communicatiedienstverlener krachtens artikel 126n ev. WvSv.

van de politie die zijn aangesteld voor de uitvoering van de politietaak verstrekken, wederom voor zover er gericht naar deze gegevens is gevraagd.[75]

Vaarwegbeheerders

Op basis van de verkregen informatie blijkt dat vaarwegbeheerders in voorkomende gevallen AIS-gegevens van particuliere bedrijven proberen te verkrijgen. Ook hiervoor geldt dat altijd moet worden bepaald op basis van welke grondslag en voor welk doel de gegevens worden verstrekt, maar ook op basis van welke grondslag en voor welk doel de gegevens worden ontvangen door de vaarwegbeheerder.

Overige partijen

Partijen die AIS-gegevens ontvangen, kunnen door eenieder in feite benaderd worden om deze gegevens aan hen te verstrekken, of zij kunnen dit uit eigener beweging doen. Omdat de AIS-gegevens persoonsgegevens bevatten, moeten ook deze verstrekkingen en ontvangsten gebeuren op basis van de Wbp.

[75] Art. 9 lid 1 Besluit meldingsformaliteiten en gegevensverwerkingen scheepvaart: “Een ontvanger van gegevens, bedoeld in artikel 5, geeft, buiten de in artikel 8 bedoelde gevallen, slechts na een daartoe strekkend verzoek inzage in door hem ontvangen gegevens of verstrekt deze gegevens aan:
(..)
sub c: ambtenaren die bij of krachtens artikel 141 van het Wetboek van Strafvordering belast zijn met de opsporing van een strafbaar feit voor zover gericht naar gegevens wordt gevraagd;
sub d: ambtenaren van politie die zijn aangesteld voor de uitvoering van de politietaak voor zover gericht naar gegevens wordt gevraagd.”

7. Ontwikkelingen

Mede op basis van de mogelijkheden die AIS-gegevens bieden en de technologische ontwikkelingen, zijn er steeds meer plannen ten aanzien van AIS. Dit betreft zowel het aantal en de aard van de gegevens die moeten worden uitgezonden, alsook de toepassingen en het gebruik.

7.1 Uitbreiding lijst verplicht uit te zenden informatie via de AIS

Technisch gezien is het mogelijk om meer gegevens via de AIS te versturen, bijvoorbeeld vrachtbrieven of andere informatie over het schip. Wanneer overwogen wordt om meer gegevens verplicht via de AIS uit te laten zenden, moet in het achterhoofd worden gehouden dat de AIS-gegevens voor eenieder met de juiste ontvanger te ontvangen zijn.

Wanneer bijvoorbeeld informatie over ladingen verstuurd worden via de AIS kan dit mogelijk een aantrekkende werking hebben op criminelen. Daarnaast kan het economisch nadelige effecten hebben voor de schipper of de opdrachtgever.

7.2 Toegang tot AIS-gegevens voor transporteurs

Een andere ontwikkeling is om transporteurs vanuit logistiek oogpunt AIS-gegevens te laten ontvangen. De Nederlandse wetgever lijkt in de implementatie van de RIS-Richtijn hiervoor geen ruimte te laten in tegenstelling tot de RIS-Richtlijn. Blijkens artikel 3 sub a van de RIS-Richtlijn hebben RIS geen betrekking op interne commerciële activiteiten tussen een of meer betrokken bedrijven, maar kunnen zij wel aan commerciële activiteiten worden gekoppeld.

Zoals eerder benoemd, zouden transporteurs mogelijk wel AIS-gegevens kunnen verwerken als zij de ondubbelzinnige toestemming hebben verkregen van de schippers.

7.3 Gegevensverwerking door ILT

De Inspectie voor Leefomgeving en Transport (‘ILT’) is de hoofdtoezichthouder in de binnenvaart waarbij zij samenwerkt met lokale en provinciale partijen. De ILT is belast met het houden van toezicht op de naleving van onder meer de vastgestelde arbeidstijden.

Ten behoeve van deze naleving is de ILT bezig met het ontwikkelen van risicoprofielen. Deze profielen worden opgebouwd op basis van onder meer resultaten van inspecties uit het verleden. Het doel hiervan is om (de planning van) inspecties efficiënter te laten verlopen en om een evenredige verdeling van inspecties te creëren en daarmee de overlast voor de schipper zo veel mogelijk te beperken. Deze profielen worden bij de ILT in een eigen systeem opgeslagen. Wanneer door middel van het systeem wordt vastgesteld bij welke schepen men wil inspecteren, moet de locatie van het schip worden vastgesteld. Hiervoor zou de ILT graag gebruik maken van de locatie-informatie die wordt verkregen door middel van de AIS. De ILT wil deze informatie niet zelf opvangen maar van bijvoorbeeld vaarwegbeheerders ontvangen.

De ILT wil het locatiegegeven dat via de AIS-apparatuur wordt verkregen dus gebruiken voor toezichtsdoeleinden, wat kan leiden tot handhaving. Toezicht en handhaving vallen

echter vooralsnog buiten het doel waarvoor AIS-gegevens oorspronkelijk zijn verzameld, zoals ook in het reeds verlopen convenant was afgesproken.

Wanneer er geen rechtsgrondslag bestaat om het locatiegegeven te gebruiken, is het gebruik niet toegestaan. Dit betekent dat wanneer de ILT het locatiegegeven, verkregen door middel van een AIS, wil gebruiken voor toezichtsdoeleinden een wettelijke grondslag gecreëerd zou moeten worden.[76]

Vaarwegbeheerders kunnen op grond van artikel 8 sub e Wbp juncto artikel 43 Wbp de gegevens verstrekken aan de ILT, wanneer deze gegevens nodig zijn voor de goede uitvoering van haar publiekrechtelijke taak en het gaat om één van de situaties genoemd in artikel 43 Wbp (bijvoorbeeld opsporing strafbare feiten, of gewichtige financiële of economische belangen van de staat). Artikel 43 Wbp doorkruist dan de doelbindingsbepaling. Echter, op grond van de ons beschikbare informatie is (nog) niet vast komen te staan dat deze informatie voor de ILT daadwerkelijk noodzakelijk is. Voorts moet het dan gaan om specifieke gevallen en niet om een 'standaardverstrekking'.

Gaat het om de opsporing van strafbare feiten, dan is het juridisch kader van de ILT-IOD van toepassing. Als bijzondere opsporingsdienst is zij gebonden aan de kaders van het Wetboek van Strafvordering (zie artikel 141 Wetboek van Strafvordering) en moet zij dus ook gegevens vorderen waar van toepassing.

7.4 Gezamenlijke walinfrastructuur

Uit de gesprekken is gebleken dat er plannen zijn van RWS en de Kustwacht om een gezamenlijk walinfrastructuur aan te leggen voor het ontvangen van AIS-gegevens rondom het IJsselmeer. Het IJsselmeer is een binnenwater en RWS is hiervoor de vaarwegmanager. Hierom lijkt de gegevensverwerking door RWS te kunnen gebeuren op basis van een publiekrechtelijke taak.

De Kustwacht heeft echter ook een bepaalde rol te spelen op het IJsselmeer, met name ten aanzien van de veiligheid, toezicht en handhaving. Het is echter de vraag of de Kustwacht een rechtsgrondslag heeft om AIS-gegevens te mogen ontvangen op het IJsselmeer. Indien de Kustwacht de gegevens mag ontvangen, is het vervolgens de vraag of de Kustwacht dezelfde gegevens en met dezelfde frequentie als RWS mag ontvangen.

Op het moment dat twee verschillende organisaties gezamenlijk het doel en middelen van een bepaalde verwerking van persoonsgegevens bepalen, zijn zij gezamenlijke verantwoordelijken. Zij zijn dan beide verantwoordelijke voor de gehele verwerking, ook als een bepaald deel van de verwerking feitelijk door de andere partij wordt gedaan. Als één van de partijen geen rechtsgrondslag voor het verwerken van de gegevens heeft, wordt in strijd met de Wbp gehandeld.

Het is daarom van belang om, voordat een gezamenlijke walinfrastructuur wordt aangelegd, ervoor te zorgen dat beide partijen ook daadwerkelijk de AIS-gegevens nodig hebben voor

[76] https://www.ilent.nl/onderwerpen/transport/binnenvaart/index.aspx.

het doel waarvoor ze deze willen verwerken en dat ze een grondslag hebben. Daarnaast moeten ze ook heldere afspraken maken over de onderlinge relatie.

8. Analyse privacyvraagstukken AIS

AIS-gegevens zijn onder omstandigheden te kwalificeren als persoonsgegevens. In de binnenscheepvaart zullen AIS-gegevens in de meeste omstandigheden worden gekwalificeerd als persoonsgegevens, omdat de relatie tussen het schip en de schipper (en diens gezin) in de meeste gevallen een 1-op-1-relatie is.

AIS-gegevens geven inzicht in de persoonlijke levenssfeer van de schipper, meer specifiek diens locatie. Deze informatie kan door derden worden gebruikt of misbruikt. Zo kunnen criminelen zien waar een binnenvaartschipper zich bevindt, of kan de ILT een compleet beeld krijgen van het gedrag van een schipper. Tegenover de privacy-schendingen staan maatschappelijke belangen. Of het privacybelang van de schipper zwaarder weegt dan het belang van een derde zal per geval moeten worden bekeken.

Privacyrisico's bij het gebruik van AIS ontstaan grofweg in de volgende situaties:

1) Ontvangst en het hierop volgende gebruik van AIS-gegevens door onbevoegde derden;
2) Hergebruik van AIS-gegevens door bevoegde partijen voor andere doelen dan waarvoor de gegevens oorspronkelijk zijn verzameld en bedoeld.

Ad 1) Onbevoegde ontvangst en gebruik
Wanneer onbevoegde derden (partijen die geen juridische grondslag hebben in de Wbp voor het verwerken van AIS-gegevens) AIS-gegevens krijgen en gebruiken, ontstaan privacyrisico's. AIS-gegevens kunnen door onbevoegde derden op twee manieren worden ontvangen:

1) zij ontvangen de AIS gegevens zelf via een VHF-ontvanger;
2) zij ontvangen AIS-gegevens van derden die deze gegevens in een eerder stadium (al dan niet bevoegd) hebben ontvangen.

De kans dat onbevoegde derden AIS-gegevens ontvangen, is groot gezien de technische keuzes die zijn gemaakt bij het inrichten van AIS in Nederland. De keuze voor VHF-ontvanger en -zenders in plaats van AI-IP voor het uitzenden van AIS-gegevens bergt een inherent privacy-risico in zich: iedereen met een geschikte ontvanger is in staat om de gegevens te ontvangen. Hier staat de robuustheid van de VHF-infrastructuur tegenover.

Wil men de privacy van binnenschippers beter beschermen dan is een overstap naar een beveiligd systeem, zoals wellicht een AI-IP infrastructuur, de meeste effectieve oplossing (omdat men de gegevens dan niet meer zomaar kan ontvangen), maar dit betekent mogelijk wel concessies aan de robuustheid van het systeem naast hoge vervangingsinvesteringen.[77]

[77] Considerati is als juridische dienstverlener niet in staat om de commerciële en technische haalbaarheid van AI-IP te beoordelen en eigenstandig een kosten-baten analyse te maken in relatie tot AIS.

Onbevoegde derden kunnen AIS-gegevens ook krijgen van anderen die deze gegevens in een eerder stadium hebben ontvangen. Dit probleem kan aan de kant van de vaarwegbeheerders worden geadresseerd door duidelijke regels op te stellen omtrent het beschikbaar stellen van AIS-gegevens aan derden. Deze derden moeten altijd een rechtmatige grondslag op grond van de Wbp kunnen aantonen alvorens zij de gegevens mogen ontvangen. Voor alle andere ontvangers (bijvoorbeeld particulieren of private partijen) wordt het een stuk lastiger om hen te dwingen alleen de gegevens door te sturen met een rechtmatige grondslag. Het ligt hier meer voor de hand om de ontvangers aan te pakken die de gegevens zonder grondslag gebruiken. Ook dit tweede probleem kan deels effectief geadresseerd worden door een overschakeling naar AI-IP. Is dit niet mogelijk, dan moet de oplossing worden gezocht in de handhaving tegen deze derde partijen.

Ad 2 Hergebruik van AIS-gegevens
Vaarwegbeheerders en andere bevoegde partijen die AIS-gegevens ontvangen voor vaarwegmanagement doeleinden kunnen deze gegevens ook gebruiken voor ‘verenigbare doelen’. Wat evenwel verenigbaar is, moet van geval tot geval beoordeeld worden op basis van de eerder in deze rapportage genoemde criteria.

9. Conclusie

In dit rapport is de vraag besproken in hoeverre er sprake is van schending van de privacy indien AIS-gegevens worden doorgegeven en bijvoorbeeld gepubliceerd worden op Internet?

Daarnaast is ingegaan op de vragen in hoeverre deze gegevens door de vaarwegbeheerders (en wellicht anderen) nog voor andere, niet in de wet gespecificeerde doelen, gebruikt worden en in hoeverre deze gegevens worden doorgegeven aan derden, voor welke doelen en met welke grondslag? Hierbij is ook gekeken of voldoende gewaarborgd is dat de gegevens niet voor andere doelen worden gebruikt?

Zoals in het tweede hoofdstuk is behandeld, moeten schepen wanneer zij om binnenvaarwegen varen de AIS-gegevens uitzenden. Deze AIS-gegevens zijn door middel van een VHF-ontvanger die op de juiste frequentie is afgesteld door eenieder te ontvangen. De gegevens worden niet-versleuteld verstuurd. Zowel het Wetboek van Strafrecht, als ook de Wbp stellen echter beperkingen aan het mogen ontvangen van de informatie die wordt uitgezonden via AIS-apparaten. Dit laat onverlet dat de gegevens in de praktijk wel degelijk worden ontvangen en gebruikt.

Het is hierbij van belang om te erkennen dat schippers worden verplicht de gegevens onversleuteld uit te zenden. Dit betekent dat het systeem dat gekozen is niet privacy-vriendelijk is. Door de voortschrijding van de techniek zou door de wetgever kunnen worden overwogen of de verplichting om bepaalde gegevens door schippers te laten uitzenden ten behoeve van het vaarwegbeheer op een privacy-vriendelijker manier kan worden ingevuld.

Gebruik door vaarwegbeheerders

Voor wat betreft vaarwegbeheerders geldt dat zij voor het doel van verkeersmanagement de persoonsgegevens die door de AIS-apparaten worden uitgezonden, mogen verwerken op basis van hun publiekrechtelijke taak.

Er heerst echter veel onduidelijkheid over wat er precies onder de taak van het verkeersmanagement valt. Bij de relevante partijen bestaan hierover verschillende meningen. Het is belangrijk om hier meer helderheid over te geven.

Ook is het van belang om duidelijke bewaartermijnen vast te stellen en om deze ook na te leven. Op dit moment lijkt het erop dat er slechts beperkt termijnen zijn vastgesteld en dat deze bewaartermijnen niet of nauwelijks worden nageleefd als ze er wel zijn.

Daarnaast moet worden vastgesteld of AIS-gegevens allemaal ongewijzigd opgeslagen moeten worden, of dat ze geanonimiseerd dienen te worden opgeslagen. Dit hangt af van het doel van de verdere verwerking. Van belang is om altijd te bepalen of het daadwerkelijk noodzakelijk is om persoonsgegevens te verwerken voor het bepaalde doel, waarbij ook de principes van proportionaliteit en subsidiariteit moeten worden meegenomen.

Het is voorts niet duidelijk bij welke partijen, personen en/of afdelingen binnen RWS als vaarwegbeheerder AIS-gegevens allemaal beschikbaar zijn. Dit is in ieder geval RWS CIV, het operationeel beheer en HAGO, maar het is niet duidelijk waar deze gegevens zich nog meer bevinden en hoe deze gegevens gebruikt worden.

Dit leidt er in het verlengde toe dat er onduidelijk heerst over de vraag wie de beslissingen neemt ten aanzien van het verwerken van de persoonsgegevens, wie er toegang mag krijgen over de gegeven en hoe lang de gegevens bewaard worden. Het wordt aanbevolen om dit voor heel RWS duidelijk vast te leggen, ook om te voorkomen dat voor toegang tot de gegevens wordt 'geshopt' bij de verschillende organisaties.

Gebruik door derden

Daarnaast hebben ook andere partijen, buiten de vaarwegbeheerders, toegang tot de AIS-gegevens. Zo zijn er een aantal private partijen, zoals Marine Traffic, vesselfinder.com en shipfinder.com, die AIS-gegevens verwerken. Het is zeer de vraag of deze verwerkingen van persoonsgegevens wel gebeuren in overeenstemming met de Wbp. Het is daarnaast ook niet duidelijk of deze organisaties de AIS-gegevens verzamelen met eigen ontvangers, of dat zij gebruik maken van particulieren die ontvangers hebben geplaatst.

Op het moment dat een organisatie persoonsgegevens verwerkt, ongeacht of de organisatie de AIS-gegevens zelf met een ontvanger verzamelt of niet, is de organisatie verantwoordelijke in de zin van de Wbp en moet de organisatie voldoen aan de vereisten in de wet. De organisatie moet dan ook een rechtsgrondslag hebben als bedoeld in artikel 8 van de Wbp. Als de persoonsgegevens zonder grondslag worden verwerkt, is de verwerking in strijd met de Wbp.

Het zou echter kunnen zijn dat de private organisatie de verwerking op basis van toestemming van de schipper(s) doet. Dan moeten schippers deze toestemming ook kunnen intrekken. Wanneer de verwerking wordt gebaseerd op het gerechtvaardigde belang van de verantwoordelijke zal er een goede belangenafweging moeten zijn gemaakt en moet de schipper verzet kunnen aantekenen. Het is niet duidelijk op basis waarvan de private partijen de persoonsgegevens verwerken.

Daarenboven geldt dat verantwoordelijken die persoonsgegevens verwerken ook aan de andere vereisten in de wet moeten voldoen. Zo moeten ze bijvoorbeeld transparant zijn over de vraag waarom de gegevens worden verwerkt, of de gegevens aan anderen worden verstrekt dan wel publiek worden gemaakt en moeten er goede beveiligingsmaatregelen worden getroffen.

Het publiceren van AIS-gegevens van binnenvaartschepen op internet betreft een verstrekking van persoonsgegevens. Een verstrekking van persoonsgegevens moet altijd worden gebaseerd op een rechtsgrondslag uit de Wbp en zal door de verantwoordelijke in kwestie moeten worden bepaald. Vaarwegbeheerders zullen in dit kader moeten nagaan of een verstrekking van persoonsgegevens, door ze publiek beschikbaar te stellen, valt binnen verkeersmanagement en dus binnen hun publiekrechtelijke taak. Indien de verantwoordelijke de grondslag 'gerechtvaardigd belang' wil gebruiken voor de

verstrekking, zal de aard en de gevoeligheid van de gegevens en de impact op de privacy van de binnenvaartschipper moeten worden meegewogen.

9.1 Aanbevelingen

Technisch

- Heroverweeg mogelijke andere systemen voor het verzenden en ontvangen van de relevante informatie tussen schepen onderling en tussen schepen en walinfrastructuur om de privacy van binnenvaartschippers te waarborgen. Hierbij moeten de voortschrijdende technische mogelijkheden worden meegenomen;
- Verwijder gegevens als deze niet meer noodzakelijk zijn voor het specifieke doel. Stel dus duidelijke bewaartermijnen vast en zorg dat deze worden nageleefd;
- Anonimiseer gegevens zoveel mogelijk, zodat wordt voldaan aan het principe van dataminimalisatie;
- Implementeer bij alle toepassingen van AIS-gegevens het principe van Privacy by Design.
- Beperk zoveel mogelijk de hoeveelheid (persoons)gegevens die door middel van AIS moeten worden uitgezonden.

Organisatorisch

- Leg helder de verantwoordelijkheid binnen de verkeersmanagement, vaarwegbeheerder en vaarwegmanagement vast ten aanzien van het verwerken van persoonsgegevens. Dit speelt met name bij RWS;
- Leg duidelijk vast wat wordt verstaan onder het doel 'vaarwegbeheer' en 'vaarwegmanagement';
- Bepaal voor elke verwerking van AIS-gegevens voor welk doel dit wordt gedaan en met welke grondslag;
- Indien de verwerking voor een ander doel is, bepaal dan of het voor een verenigbaar doel is;
- Stel een procedure op ten aanzien van de toelaatbaarheid van verstrekking van AIS-gegevens aan derde partijen.

Handhaving

- Treed in gesprek met de aanbieders van websites en apps die AIS-gegevens publiceren en laat hen aantonen op welke wettelijke basis zij de verwerking baseren;
- Indien dit op basis van het gerechtvaardigde belang is, laat ze dan hun gerechtvaardigd belang aantonen, inclusief de belangenafweging die is gemaakt;
- Kijk of het mogelijk is om (een subset van) de AIS-gegevens van binnenvaartschippers uit de getoonde dataset te halen. Denk hierbij onder andere aan contactgegevens, maar mogelijk ook aan de real-time locatie van het schip;
- Indien de derde partijen weigeren gehoor te geven aan verzoeken om privacybeschermende maatregelen te nemen, overweeg dan (gezamenlijke) handhaving met de Autoriteit Persoonsgegevens en/of het Agentschap Telecom.