Model Protocol

Afsprakenstelsel Gatekeeper 2024

voor Deelnemers in de logistieke sector in Nederland

v1.2.1

INHOUD

EXECUTIVE SUMMARY

Dit protocol weerspiegelt zorgen over veiligheid, fraude en criminaliteit bij de deelnemende bedrijven, en het voorkomen van daaruit voortvloeiende corruptie, (excessief) geweld in de publieke ruimtes, economische- en imagoschade van de getroffen bedrijven in de logistieke sector. Het benadrukt de balans tussen efficiënte toegangsmanagement en strenge beveiligingsmaatregelen tegen criminaliteit en fraude.

Het Model Protocol Afsprakenstelsel Gatekeeper helpt bij het voorkomen van criminele activiteiten bij de deelnemende bedrijven binnen de logistieke sector van Nederland, zoals (lucht)havens en transportbedrijven. Als iemand, die normaal gesproken rechtmatig toegang mag krijgen omdat hij een toegangspas heeft, verdacht gedrag vertoont dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring kan dragen, kunnen de Deelnemers besluiten om deze persoon tijdelijk de toegang tot bepaalde hoog risico locaties te beperken.

Dit alles wordt heel zorgvuldig uitgevoerd om ervoor te zorgen dat alleen de juiste informatie gebruikt wordt, hoor en wederhoor plaatsvindt en iedereen eerlijk behandeld wordt, onder meer door een toetsing op willekeur door Stichting Gatekeeper. Er zijn regels die helpen te beslissen wie toegang krijgt en wie niet. Betrokken toegangspasgebruikers kunnen bezwaar maken als ze denken dat er een fout is gemaakt.

1. **Doelstelling**: het Model Protocol Afsprakenstelsel Gatekeeper is opgezet om fraude en criminaliteit bij de deelnemende bedrijven binnen de Nederlandse logistieke sector te bestrijden, specifiek voor faciliteiten van (lucht)havens en transportbedrijven die een hoog risico hebben.
2. **Deelnemers**: het afsprakenstelsel omvat diverse (lucht)havenbedrijven en distributie- en transportbedrijven die zijn aangesloten bij Stichting Gatekeeper. Elke Deelnemer beheert een eigen, *decentraal* Incidentenregister waarin incidenten op het gebied van fraude en criminaliteit die op hun eigen faciliteiten voorkomen, worden geregistreerd.
3. **Centraal Incidentenregister**: Stichting Gatekeeper beheert namens de Deelnemers een *centraal* Incidentenregister waarin incidenten op het gebied van fraude en criminaliteit worden geregistreerd.
4. **Vergunning voor het delen van strafrechtelijke persoonsgegevens**: het delen van strafrechtelijke persoonsgegevens is onderworpen aan strikte voorwaarden, waaronder een vergunning van de Autoriteit Persoonsgegevens op grond van dit protocol.
5. **Toegangsbeperkingen**: bij gedrag dat redelijkerwijs een strafrechtelijke bewezenverklaring zou kunnen dragen, kan een toegangspasgebruiker als maatregel een tijdelijke toegangsbeperking tot verschillende hoog risico faciliteiten opgelegd krijgen. Zie voor de maatstaf de definitie van Gedragingen.
6. **Procedures en rechten**: Er zijn duidelijke procedures voor het opleggen van proportionele maatregelen en voor het bewaken van de rechten van betrokkenen, zoals een klachtenprocedure en bezwaar- en beroepsmogelijkheden.
7. **Transparantie en rechtsbescherming**: Deelnemers en Stichting Gatekeeper zijn verplicht tot transparantie tegenover Kaartgebruikers en moeten de bescherming van persoonsgegevens waarborgen.
8. **Samenwerking met autoriteiten**: er is een samenwerking met gemeentes, brancheorganisaties en vervoerders in de logistieke sector.

9. **Geautoriseerde functionarissen**: specifieke functionarissen binnen de deelnemende organisaties zijn geautoriseerd om persoonsgegevens te verwerken in overeenstemming met de AVG.
10. **Evaluatie en wijziging**: de uitvoering van het protocol wordt regelmatig geëvalueerd en kan, na goedkeuring van de AP, worden aangepast om effectiviteit en naleving van de wet- en regelgeving te verzekeren.

DEFINITIES

Afsprakenstelsel: het waarschuwingssysteem Gatekeeper voor Deelnemers dat bestaat uit het Centraal Incidentenregister Gatekeeper, de (decentrale) Incidentenregisters van elk van de Deelnemers en de toegangsmanagementsystemen van Identiteitsproviders;

AP: de Autoriteit Persoonsgegevens;

AVG: de Algemene Verordening Gegevensbescherming;

Centraal Incidentenregister Gatekeeper: de deelverzameling van het Incidentenregister van een Deelnemer dat uitsluitend verwijzingsgegevens bevat met betrekking tot (rechts)personen en dat bestemd is voor gebruik door alle Deelnemers en Stichting Gatekeeper;

Commissie van Beroep: commissie die het beroep behandelt dat een Kaartgebruiker indient tegen een Maatregel, opgelegd door Stichting Gatekeeper en bevestigd door de Geschillencommissie. De Commissie van Beroep handelt conform dit protocol en het reglement van de Commissie van Beroep;

Deelnemer: een (lucht)havenbedrijf of een distributie- of transportbedrijf in de logistieke sector dat deelneemt aan project Gatekeeper door het onderschrijven van dit protocol en dat de algemene, of voor zijn rol specifiek geldende voorwaarden van Stichting Gatekeeper heeft ondertekend;

Dienstverlener: organisatie die werkzaamheden op een faciliteit verricht;

Faciliteit: een gebouw, terrein of locatie van een Deelnemer in Nederland waar goederen aankomen vanuit het buitenland of vertrekken naar het buitenland;

Geautoriseerde functionaris: de persoon binnen de organisatie van een Deelnemer die in het kader van zijn taakuitoefening gerechtigd is om gegevens te delen met het Centraal Incidentenregister Gatekeeper en, indien nodig, deze gegevens zal beoordelen. Hieronder vallen ook afgevaardigde medewerkers van de Deelnemers die Stichting Gatekeeper om advies vragen bij beoordelingen, of om plaats te nemen in de Geschillencommissie of de Commissie van Beroep[1];

Gedragingen: gedrag van een Kaartgebruiker dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van artikel 350 van het Wetboek van Strafvordering - kunnen dragen. De vastgestelde gedragingen moet een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan[2] aan de hand van bewijsmiddelen, zoals camerabeelden en getuigenverklaringen, en de overtuiging dat het gedrag is vertoond door de Kaartgebruiker, waarbij geen reële ruimte is voor alternatieve verklaringen waarin de Kaartgebruiker níet

[1] Het gaat hierbij niet om een willekeurige beveiliger maar, bijvoorbeeld in de havens, om een Port Facility Security Officer van een Deelnemer (PFSO) met een diploma Haven PFSO opleiding, of een Security Officer of Security manager. In de luchthavens en de logistieke sector gaat het om een Security Officer of Security manager. Per Deelnemer worden twee Geautoriseerde functionarissen benoemd om een single point of failure te voorkomen.

[2] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4

als degene die het gedrag heeft vertoond valt aan te merken en welk strafbaar feit het bewezen verklaarde volgens de wet zou opleveren.

Geschillencommissie: de commissie van Stichting Gatekeeper die geschillen en klachten van Kaartgebruikers behandelt conform dit protocol en het Reglement Geschillencommissie;

Hoog risico faciliteit: een gebouw, terrein of locatie van Nederlandse (lucht)havens en distributie- en transportbedrijven binnen de Nederlandse logistieke sector waar producten worden vervoerd uit regio's die een hoog risico hebben in de uitvoer of doorvoer van illegale producten (waaronder drugs), zoals Zuid-Amerika, West-Azië en Noord-Afrika, of naar regio's die een hoog risico hebben op de uitvoer of doorvoer van illegale producten (zoals drugs) binnen of vanuit Nederland. Hierbinnen vallen in ieder geval de faciliteiten van de zeehavens van Amsterdam, Delfzijl/Eemshaven, Rotterdam en Vlissingen/Terneuzen, luchthaven Schiphol en distributie- en transportbedrijven die worden gebruikt voor uitvoer en doorvoer. Stichting Gatekeeper zal op haar website www.stichtinggatekeeper.nl een (niet uitputtende) lijst publiceren van Hoog risico faciliteiten waar het Afsprakenstelsel van toepassing is;

Identiteitsprovider: De organisatie die persoonsgebonden toegangspassen verstrekt en persoonsgegevens valideert ten bate van de toegangsverlening tot de faciliteiten van Deelnemers;

Incident: een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad waarbij de belangen, integriteit of veiligheid van de medewerkers van een Deelnemer, de Deelnemer zelf, Stichting Gatekeeper of de logistieke sector als geheel in het geding zijn of kunnen zijn;

Incidentenregister: de decentrale gegevensverzameling(en) van een Deelnemer, waarin gegevens zijn vastgelegd naar aanleiding van, of betrekking hebbend op een (mogelijk) Incident;

Integriteitsovereenkomst: de overeenkomst tussen de Deelnemers, Stichting Gatekeeper en de Kaartgebruiker. De Integriteitsovereenkomst bevat de gezamenlijke Gatekeper community gedragsregels;

Kaartgebruiker: een persoon die werkzaamheden uitvoert voor of namens een Deelnemer en daarom van een Deelnemer rechtmatig toegang heeft verkregen tot faciliteiten van een Deelnemer. Hiervoor heeft een Deelnemer aan Kaartgebruiker een (digitale) toegangspas ter beschikking gesteld uitsluitend ten behoeve van het uitvoeren van werkzaamheden voor of namens een Deelnemer.;

Maatregel: een proportionele beperking van toegang tot Hoog risico faciliteiten van meerdere Deelnemers opgelegd aan een Kaartgebruiker naar aanleiding van Gedragingen (van die Kaartgebruiker) zoals hierboven gedefinieerd;

Persoonsgegeven: zoals bepaald in de AVG;

Stichting Gatekeeper: organisatie die ten behoeve van de Deelnemers de toegang van personen tot de Hoog risico faciliteiten tijdelijk kan beperken;

Strafrechtelijk persoonsgegeven: persoonsgegevens van strafrechtelijke aard als bedoeld artikel 1 UAVG en artikel 10 AVG;

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming;

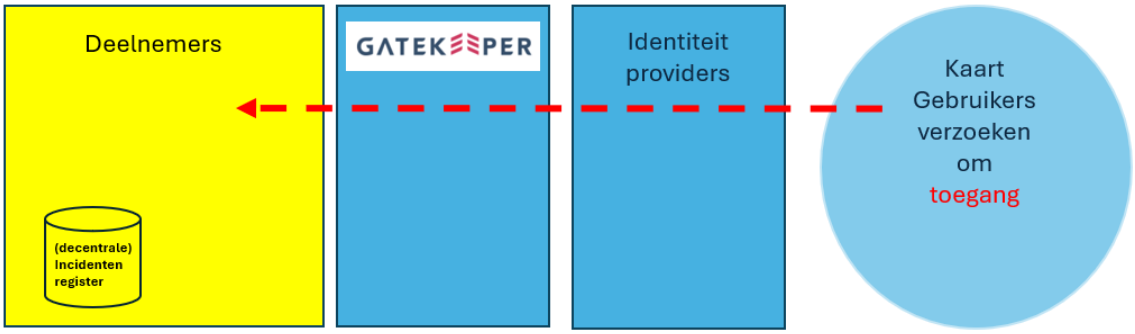
Verwerkingsverantwoordelijke: zoals bepaald in de AVG;

Verwerker: zoals bepaald in de AVG;

Verwerkersovereenkomst: een overeenkomst conform artikel 28 AVG.

1. BESCHRIJVING AFSPRAKENSTELSEL GATEKEEPER

De keten van het Afsprakenstelsel wordt weergegeven in onderstaande figuur:



Waarom een Afsprakenstelsel?

Doel

Het doel van het Afsprakenstelsel is het bestrijden van fraude en criminaliteit bij de Deelnemers, en het voorkomen van daaruit voortvloeiende corruptie, het beschermen van de veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de Deelnemers, het voorkomen van (excessief) geweld in de publieke ruimtes, en het voorkomen van economische- en imagoschade van de getroffen bedrijven[3]. Het Afsprakenstelsel waarborgt de veiligheid door middel van onderzoek, toegangscontroles, informatie-uitwisseling over Incidenten, beoordeling van gedragingen en (indien noodzakelijk) uitvoering van een Maatregel. Deelnemers blijven de mogelijkheid houden om voor hun eigen Faciliteiten hun eigen decentrale Incidentenregister bij te houden en om hun eigen maatregelen te nemen op grond van de uitzondering zoals gesteld in artikel 33 lid 2 Uitvoeringswet AVG. Echter, zoals hieronder blijkt, is een maatregel die beperkt is tot één Faciliteit vaak niet voldoende en is er de roep om een gezamenlijk afsprakenstelsel.

Waarom?

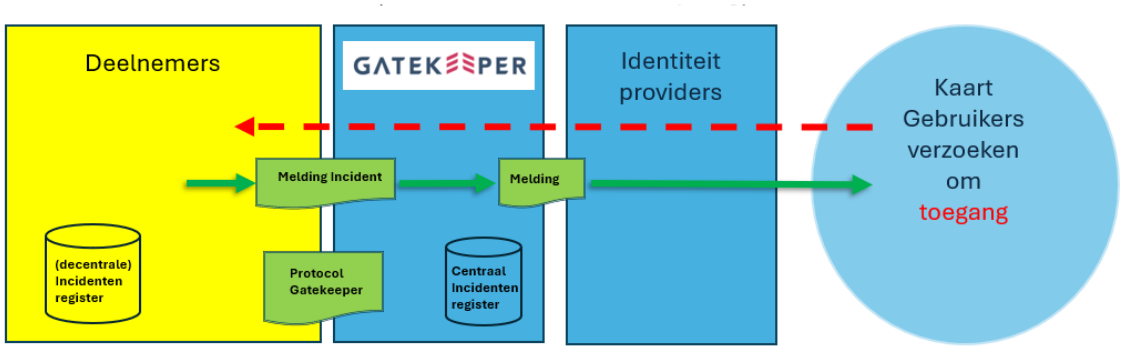
Wat klassieke mainports betreft, bijvoorbeeld zeehavens van Amsterdam, Delfzijl/Eemshaven, Rotterdam en Vlissingen/Terneuzen en luchthaven Schiphol, wordt onderkend dat georganiseerde criminelen systematisch goederenstromen benutten. Deze mainports treffen tal van security-maatregelen en beschikken over een uitgebreide publiek-private veiligheidsorganisatie. Met toezicht, handhaving, (douane)controles, opsporingsactiviteiten en toegangscontroles dragen deze professionals zorg voor de dagelijkse mainport-veiligheid. Dit contrasteert met de distributie en transportbedrijven. Zij bevinden zich in de tweede linie, op fysieke afstand van (controles aan) de EU-grens. Er is een bescheiden private veiligheidsorganisatie en de overheid was en is niet systematisch (dagelijks) aanwezig op deze locaties. Er is vrije toegang tot de terreinen. Drugs of andere illegale zaken die via een zeehaven of luchthaven (over de EU-grens) naar Nederland komen, of die hier zijn geproduceerd, kunnen worden doorgevoerd, onder meer via vervoer over de weg. De logistieke keten in bijvoorbeeld de sierteeltsector maakt als mainport in

[3] Bedrijven en opsporingsdiensten werken bijvoorbeeld in de Rotterdams haven samen om criminaliteit tegen te gaan, onder meer in het programma 'Integere Haven'. Zie ook: https://www.nederlandtegengeorganiseerdemisdaad.nl/actueel/verhalen-uit-de-praktijk/weblog/2022/overheid-en-bedrijven-gaan-in-rotterdamse-haven-georganiseerde-criminaliteit-te-lijf

de tweede linie, vanwege massale dagelijkse bloemenimport van buiten én binnen de EU, ook deel uit van de kansenstructuur die de fysieke infrastructuur in Nederland biedt voor internationale (drugs)criminaliteit[4]. Criminelen proberen regelmatig toegang te krijgen tot Faciliteiten van verschillende Deelnemers door bijvoorbeeld gebruik te maken van de toegangspas van henzelf of van een ander, of door listige kunstgrepen. Zij hebben onder meer tot doel om illegaal ingevoerde drugs uit te halen of door te voeren op de Hoog risico faciliteiten van havens, luchthavens en distributie- en transportbedrijven in de logistieke (import)keten. Personen die misbruik maken van het logistieke stelsel beperken hun activiteiten zelden tot een enkele Deelnemer. Denk hierbij aan ongeveer 20 zeehaventerminals en verschillende bedrijven op (lucht)havens en distributie- en transportbedrijven die importeren en vervoeren via Hoog risico faciliteiten. Als een poging mislukt proberen criminelen het opnieuw bij een andere Deelnemer. Ook bij een geslaagde poging bestaat het risico op herhaling bij een andere Deelnemer. Deze fraude en criminaliteit stoppen niet bij de kade, luchthaven of het transportbedrijf. Het effect is tot diep in de maatschappij te voelen en raakt de gehele Nederlandse maatschappij.

Bedrijven die binnen bijvoorbeeld de (lucht)havens opereren, hebben afgescheiden gebieden (Faciliteiten) ingericht. Hierdoor is het mogelijk de toegang genuanceerd te beheren binnen hun bestaande infrastructuur. Deze afgescheiden gebieden hebben verschillende risicoprofielen. Bedrijven beheren zelf de toegang tot deze Faciliteiten. Om in aanmerking te komen voor een toegangspas stellen de bedrijven verschillende vereisten, zoals bepaalde diploma's of certificaten ('attributen'). De toegangspas is gekoppeld aan een toegangsmanagementsysteem. Identiteitsproviders dragen zorg voor het beheer van de toegangspassen, het laden van de attributen, de verificatie van de attributen en voor de koppeling met het toegangsmanagementsysteem. Deze werkwijze is ook mogelijk in de distributie- en transportketen binnen de logistieke sector in Nederland. Stichting Gatekeeper maakt gebruik van de bestaande infrastructuur van toegangsmanagementsystemen die al door bedrijven wordt gebruikt.

Rol Stichting Gatekeeper



Stichting Gatekeeper heeft ten doel het tegengaan van fraude en georganiseerde ondermijnende (drugs)criminaliteit in Hoog risico faciliteiten van haar Deelnemers, zo nodig op meerdere faciliteiten tegelijkertijd. Dit doet Stichting Gatekeeper in samenwerking met Deelnemers, gemeenten, brancheorganisaties en vervoerders in de logistieke sector en door het bijhouden van een Centraal Incidentenregister namens de Deelnemers. Deze opzet past onder meer binnen de versterkte aanpak van de bescherming van de vitale

[4] 'Een Pact voor de Rechtsstaat. Een sterke terugdringing van drugscriminaliteit in tien jaar', Noordanus, 2020, Den Haag.

infrastructuur van het ministerie van Justitie[5]. De overheid probeert strafrechtelijke interventies te verbinden aan het verstoren van logistieke processen, het opwerpen van barrières en het ontwikkelen van preventieve slagkracht, maar deze verschillende sporen laten zich in de praktijk niet altijd even gemakkelijk koppelen[6]. Omdat bedrijven al verplicht zijn om in hun bedrijfsbeveiligingsplan verschillende technische en organisatorische maatregelen te nemen om de beveiliging van hun terreinen te waarborgen, vormt het Afsprakenstelsel en het toegangsmanagement via Gatekeeper het sluitstuk op de technische en organisatorische maatregelen die bedrijven gebruiken om barrières op te werpen tegen criminaliteit en fraude. De rol van Stichting Gatekeeper is dat zij faciliteert dat centrale registratie plaatsvindt van welke Kaartgebruikers wel of geen toegang mogen hebben tot de Hoog risico faciliteiten van de aangesloten Deelnemers. Ook beheert Stichting Gatekeeper de Persoonsgegevens die de Deelnemers met haar delen, conform de voorwaarden van dit protocol.

Middelen

Samen met de overheid en het bedrijfsleven maken én houden Stichting Gatekeeper en haar Deelnemers het werk binnen de Hoog risico faciliteiten van de Deelnemers voor iedereen veiliger. Het Afsprakenstelsel Gatekeeper gebruikt hiervoor het toegangsbewijs van het toegangsmanagementsysteem binnen de infrastructuur die de Deelnemers al gebruiken. Stichting Gatekeeper coördineert, in overleg met de Deelnemers, het onderzoek, de toegangscontroles, de informatie-uitwisseling over Incidenten, de centrale registratie van Incidenten en waar nodig de uitvoering van Maatregelen. Wanneer er regels worden overtreden sluit het Afsprakenstelsel Gatekeeper de poort voor die specifieke Kaartgebruiker. Immers, alle medewerkers binnen de faciliteiten van Deelnemers hebben het recht op een veilige werkomgeving.

Waarborgen

In dit protocol wordt beschreven dat de gegevensuitwisseling in het kader van dit protocol plaatsvindt op een beveiligde manier plaats zal vinden tussen de Geautoriseerde functionaris van de veiligheidsafdelingen van de betreffende Deelnemer en het Centraal Incidentenregister Gatekeeper. Andere waarborgen zijn dat alleen de Geautoriseerde functionaris van de betreffende Deelnemer bevoegd is tot het nemen van beslissingen over de melding aan en het delen van gegevens over Incidenten aan het Centraal Incidenten Register Gatekeeper. Om willekeur te voorkomen zal Stichting Gatekeeper die melding toetsen aan dit protocol. De Geautoriseerde functionaris van de betreffende Deelnemer kan hun eigen gegevens rechtstreeks raadplegen in het eigen Incidentenregister. Verder wordt de toegang tot de gegevens adequaat beveiligd en zijn op de verzameling en uitwisseling de beginselen van proportionaliteit en subsidiariteit van toepassing. Bij de verwerking van Persoonsgegevens wordt zoveel mogelijk transparantie ten opzichte van de Kaartgebruiker betracht, Persoonsgegevens worden niet langer bewaard dan noodzakelijk en Stichting Gatekeeper heeft een laagdrempelige geschillenregeling ingericht. Tot slot is zij een onafhankelijke coördinator tussen de Deelnemers en de genoemde instanties en fungeert zij als kenniscentrum dat waarborgt dat een Maatregel conform dit protocol wordt toegepast.

---

[5] https://www.rijksoverheid.nl/documenten/kamerstukken/2023/05/30/tk-versterkte-aanpak-bescherming-vitale-infrastructuur

[6] Wetenschappelijk Onderzoek en Data Centrum Rijksoverheid (WODC) rapport 'Koers bepalen, over de lessen van de versterking aanpak georganiseerde drugscriminaliteit', Nelen, e.a., Erasmus Universiteit, 20 december 2022, p. 93. Te raadplegen via: https://repository.wodc.nl/handle/20.500.12832/3075

Scope is landelijk, beperkt tot de logistieke sector en Hoog risico faciliteiten in Nederland

De scope van het protocol is beperkt tot de logistieke sector in Nederland. Deelnemers moeten zijn aangesloten bij Stichting Gatekeeper en zijn daarmee gebonden zijn aan de toepassing van dit protocol. Het protocol richt zich op de Hoog risico faciliteiten van Deelnemers, dus locaties waar een hoog risico bestaat om slachtoffer te worden van fraude en georganiseerde (drugs)criminaliteit. De praktijk wijst uit dat het kwalificeren van een Hoog risico faciliteit dynamisch is. Bedrijfsontwikkelingen in het vervoer van soorten producten en van en naar regio's kunnen invloed hebben op de kwalificatie van faciliteiten. Naar verwachting zullen bedrijven die veel importeren uit hoog risicolanden eerder Deelnemer willen worden dan bedrijven die alleen binnen Nederland vervoeren.

Eén Afsprakenstelsel Gatekeeper

Voor de meest effectieve werking, wil het Afsprakenstelsel zo veel mogelijk (lucht)havenbedrijven en distributie- en transportbedrijven in de logistieke sector aan te laten sluiten. . De verschillende Deelnemers maken gebruik van de diensten van verschillende Identiteitsproviders. Die Identiteitsproviders kennen in hun toegangsmanagementsysteem het attribuut 'Gatekeeper' toe. Als dat nodig is, vraagt Stichting Gatekeeper aan de Identiteitsproviders om dit attribuut uit te zetten voor een specifieke Kaartgebruiker, waardoor deze niet langer toegang heeft tot (een of) meerdere specifieke Hoog risico faciliteit(en) van de Deelnemers.

Hoog risico faciliteit

De beoordeling of een Faciliteit van een Deelnemer zich kwalificeert als een Hoog risico faciliteit wordt in het algemeen gebaseerd op de bekende methode van kans x impact. Nadere invulling vindt plaats door een risicoanalyse, uitgevoerd door de Deelnemer in het kader van zijn beveiligings- en veiligheidsplan[7]. Echter, de kwalificatie is geheim omdat beveiligings- en veiligheidsplannen niet openbaar zijn (anders zouden criminelen gemakkelijk precies kunnen achterhalen waar zwakke plekken in de beveiliging zitten). Vanwege deze geheimhouding definieert Stichting Gatekeeper **Hoog risico faciliteiten** in verband met dit protocol zoals weergegeven in de lijst met definities.

Criteria rond het opleggen van een Maatregel

Een Maatregel zal worden opgelegd als een Kaartgebruiker zich zo gedraagt dat die gedraging kwalificeert als een Gedraging, zoals hierboven gedefinieerd: "gedrag van een Kaartgebruiker dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van artikel 350 van het Wetboek van Strafvordering - kunnen dragen. De vastgestelde gedragingen moet een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan[8] aan de hand van bewijsmiddelen, zoals camerabeelden en getuigenverklaringen, en de overtuiging dat het gedrag is vertoond door de Kaartgebruiker, waarbij geen reële ruimte is voor alternatieve verklaringen waarin de Kaartgebruiker níet als degene die het gedrag heeft vertoond valt aan te merken en welk strafbaar feit het bewezen verklaarde volgens de wet zou opleveren". De bewijsverzameling van Gedragingen door een Deelnemer richt zich

[7] Specifiek met betrekking tot zeehavens eisen toezichthouders zoals Havenbedrijf Amsterdam, Havenbedrijf Rotterdam, Groningen Seaports en North Sea Ports van havenbedrijven dat zij een Port Facility Security Assessment (PFSA) uitvoeren. Daarbij rekening houdend met alle risico's op verstoring van de bedrijfsprocessen, de (impact op de) omgeving en/of keten. De havenbedrijven dienen Maatregelen te treffen om criminele en ondermijnende handelingen te beperken of beheersbaar te maken.

[8] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4

vooral op gedrag dat specifiek duidt op het overtreden van de integriteitsregels 2 t/m 4 van de Integriteitsovereenkomst tussen de Deelnemers en de Kaartgebruiker:

2. *Ik betreed de faciliteiten alleen op basis van een gerechtvaardigd en legaal doel;*
3. *Ik voer geen onrechtmatige handelingen uit en zal terstond melding maken zodra ik kennis neem van of betrokken dreig te raken bij fraude, criminele activiteiten of zaken die de veiligheid op de faciliteiten beïnvloeden;*
4. *Ik breng geen mensen of goederen op het terrein die niet op het terrein horen;*

In verband met hoor en wederhoor krijgt de Kaartgebruiker tijdens het onderzoek de gelegenheid zijn visie op de feiten te geven. De Kaartgebruiker heeft bovendien het recht van klacht, bezwaar en beroep.

Belang Kaartgebruiker

De verwerking van strafrechtelijke persoonsgegevens raakt de persoonlijke levenssfeer van de Kaartgebruiker en vereist daarom bijzondere terughoudendheid. Strafrechtelijke persoonsgegevens zijn gevoelig en kunnen, indien onzorgvuldig verwerkt, leiden tot stigmatisering en uitsluiting, bijvoorbeeld bij sollicitaties of werk. De Kaartgebruiker heeft er bovendien een belang bij om niet blijvend geconfronteerd te worden met fouten uit het verleden, in het licht van het fundamentele recht op rehabilitatie en een nieuw begin.

Dit recht van betrokken Kaartgebruikers vindt zijn basis in een samenhang van rechtsbronnen, zoals het Europees Verdrag voor de Rechten van de Mens (EVRM), de AVG en het Nederlands strafrecht. Artikel 8 EVRM biedt bescherming van het privéleven, waaronder de ontwikkeling van identiteit en reputatie valt. Het Europees Hof voor de Rechten van de Mens heeft benadrukt dat langdurige opslag en verspreiding van strafrechtelijke gegevens zonder duidelijke noodzaak in strijd kan zijn met dit artikel[9]. Daarnaast vloeit uit de AVG een aantal beginselen voort die het recht op een nieuw begin ondersteunen, zoals het beginsel van dataminimalisatie, opslagbeperking en het recht op gegevenswissing. Verder is binnen het Nederlands strafrechtstelsel het beginsel van resocialisatie leidend: ex-veroordeelden dienen een reële kans te krijgen op maatschappelijke herintegratie, zonder onevenredige nadelige gevolgen van hun strafverleden. Onnodige of onevenredige verwerking van strafrechtelijke persoonsgegevens zou de ontwikkeling van identiteit en reputatie van de Kaartgebruiker kunnen beperken, en zou risico's met zich mee kunnen brengen op misbruik of datalekken, met mogelijke reputatieschade als gevolg. Om dit te voorkomen, zal de verwerking van strafrechtelijke persoonsgegevens steeds worden getoetst aan dit protocol en de beginselen van de AVG, waaronder doelbinding, proportionaliteit en subsidiariteit. De Deelnemers zullen zich houden aan de vergunning van de Autoriteit Persoonsgegevens en dit protocol, waarin strenge waarborgen zijn opgenomen voor een veilige verwerking.

Welke Maatregel zal worden genomen?

Een Deelnemer zal zelfstandig beslissen om de Kaartgebruiker de toegang tot zijn eigen Faciliteiten te beperken op grond van artikel 33 lid 2 Uitvoeringswet AVG.

Wanneer uit het onderzoek blijkt dat het gedrag kwalificeert als Gedragingen, meldt de Deelnemer dit bij Stichting Gatekeeper. Om willekeur te voorkomen zal Stichting

[9] M.M. - het Verenigd Koninkrijk (EHRM 13 november 2012, nr. 24029/07)

Gatekeeper die melding toetsen aan dit protocol. De melding leidt vervolgens tot een beperking van de toegang van deze Kaartgebruiker tot alle Hoog risico faciliteiten van alle Deelnemers. De standaard periode is 3 maanden. Voor het opleggen van een Maatregel wordt gebruik gemaakt van de toegangsmanagementsystemen van de Identiteitsproviders (sub verwerkers) waar de Deelnemers gebruik van maken.

Hiermee voorkomen de Deelnemer en Stichting Gatekeeper dat deze persoon toegang krijgt tot Hoog risico faciliteiten van de andere Deelnemers. De overige Deelnemers krijgen geen melding dat Stichting Gatekeeper een Kaartgebruiker tijdelijk de toegang tot Hoog risico faciliteiten ontzegt, tenzij de Deelnemer zelf om toegangsbeperking in het kader van Gatekeeper heeft verzocht. Alleen de Kaartgebruiker krijgt per e-mail een melding dat zijn toegang tot Hoog risico faciliteiten zal worden beperkt. Daarnaast krijgt de Kaartgebruiker aan de poort de melding dat de toegang is geweigerd met (niet meer dan) een e-mailadres voor informatie.

Na 3 maanden wordt, op basis van de dan bekend zijnde gedragingen en feiten, beoordeeld of de Maatregel wordt opgeheven. Als daar aanleiding toe is, zal de periode worden verlengd met nog eens 3 maanden. Zo nodig zal worden afgeweken van de standaard met een periode van 1 tot 6 maanden. Belangrijke aanwijzingen hierbij zijn de vraag of er nieuwe feiten naar boven zijn gekomen die een nuancering of een verlenging billijken. Als het politieonderzoek nog loopt, zal de Maatregelen met 3 maanden worden verlengd. De beperking van toegang wordt opgeheven wanneer uit de feiten blijkt dat een beperking niet langer proportioneel is. Wanneer een Kaartgebruiker meer dan een keer is veroordeeld voor fraude of drugscriminaliteit zal de Maatregel 5 jaar duren. We haken hierbij aan bij de terugkijktermijn van 5 jaar van Haven VOG. Uiteraard staat de klacht-, geschil- en beroepsprocedure open voor deze Kaartgebruikers, bijvoorbeeld als er nieuwe feiten naar boven komen.

Wanneer uit onderzoek blijkt dat gedrag van een bestuurder[10] van een bedrijf kwalificeert als Gedragingen, zal een Maatregel worden opgelegd voor het hele bedrijf, inclusief de Kaartgebruikers van dit bedrijf omdat dit hele bedrijf met zijn medewerkers een hoog risico voor de andere Deelnemers is. Stichting Gatekeeper zal de betreffende Kaartgebruikers hiervan vooraf inlichten, met vermelding van de mogelijkheden voor klacht, bezwaar en beroep.

Welke gevolgen heeft een Maatregel voor de Kaartgebruiker?

Door het opleggen van een Maatregel zal de Kaartgebruiker tijdelijk geen toegang meer krijgen tot de Hoog risico faciliteiten van alle Deelnemers. Omdat dit beperkt is tot Hoog risico faciliteiten, blijven er nog veel (lucht)havens of andere sectoren in Nederland over waar de Kaartgebruiker nog wel toegang toe krijgt en zijn logistieke diensten kan vervolgen. Voordat een Maatregel wordt opgelegd, weegt de Deelnemer de belangen van de Kaartgebruikers enerzijds en de belangen van de logistieke sector om fraude en criminaliteit te voorkomen en de veiligheid op de Hoog risico faciliteiten te waarborgen anderzijds, af.

Stichting Gatekeeper zal op haar website www.stichtinggatekeeper.nl een (niet uitputtende) lijst publiceren van Hoog risico faciliteiten waar het Afsprakenstelsel van toepassing is. De Kaartgebruiker bij wie Stichting Gatekeeper een Maatregel heeft opgelegd, kan zo zien op welke plaatsen hij nog wel zou kunnen werken.

[10] Zoals geregistreerd in het handelsregister van de kamer van koophandel.

Nuancering Maatregel

Indien de Maatregel in een specifiek geval te zwaar zou zijn voor een Kaartgebruiker (dit kan bijvoorbeeld blijken uit de hoor en wederhoor, het bezwaar of de beroepsprocedure) zal de Maatregel genuanceerd worden. Bijvoorbeeld door de Kaartgebruiker tijdelijk de toegang tot Hoog risico faciliteiten van *een bepaald aantal* Deelnemers te beperken en/of om de periode te verkorten.

De toegang bij de Deelnemers wordt geregeld via toegangsmanagementsystemen die (digitale) toegangskaarten van verschillende Identiteitsproviders gebruiken. Met behulp van de toegangsmanagementsystemen van deze Identiteitsproviders zal een Maatregel genuanceerd aan een Kaartgebruiker opgelegd kunnen worden. Na het opleggen van een Maatregel, kunnen Kaartgebruikers nog steeds aan de slag in de transportsector bij alle faciliteiten die niet de kwalificatie Hoog risico faciliteit hebben, bijvoorbeeld groenten vervoeren vanuit Zuid Holland, fruit vervoeren vanuit de Betuwe of varkens vervoeren vanuit Noord Brabant.

Beëindigen Maatregel

Er bestaan verschillende mogelijkheden en redenen om de Maatregel te beëindigen. Via de klacht, geschil- en beroepsprocedure bij Stichting Gatekeeper zal hoor en wederhoor plaatsvinden. Indien uit de door de Kaartgebruiker aangedragen bewijsvoering en verklaringen zou blijken dat het gedrag bij nader inzien toch niet kwalificeert als Gedragingen, zal de Maatregel worden beëindigd. Daarnaast zal de Maatregel centraal worden beëindigd wanneer (i) het Openbaar Ministerie en politie[11] een verdachte Kaartgebruiker berichten dat er sprake is van een afdoening (denk hierbij aan situaties als sepot[12], ontslag van rechtsvervolging, vrijspraak of dat de Kaartgebruiker zijn straf heeft uitgezeten), (ii) de Kaartgebruiker vervolgens zo'n bericht over afdoening heeft gedeeld met Stichting Gatekeeper en tenslotte (iii) Stichting Gatekeeper dit heeft besproken met degenen die verantwoordelijk zijn voor het betreffende dossier en zij van oordeel zijn dat de Maatregel dient te worden opgeheven. Stichting Gatekeeper zal zelf de strafrechtelijke persoonsgegevens verwijderen uit het dossier in het Centraal Gatekeeper Incidentenregister.

Stichting Gatekeeper zal in dat geval de Deelnemer die de initiële melding heeft gedaan, adviseren om ook de strafrechtelijke persoonsgegevens van de betreffende Kaartgebruiker te verwijderen uit het eigen Incidentenregister. Het is slechts een advies, de Deelnemer die de initiële Gedragingen heeft gemeld, mag voor zijn eigen decentrale incidentenregister zijn eigen afweging maken conform artikel 10 AVG jo 33 lid 2 UAVG.

[11] OM en politie maken hierbij gebruik van bestaande procedures onder hun wettelijke taak.

[12] De meest voorkomende redenen voor een sepot zijn: ten onrechte als verdachte aangemerkt, onvoldoende bewijs, ander dan strafrechtelijk ingrijpen prevaleert, gering feit, gering aandeel in het feit, recente bestraffing, schikking.

2. PERSOONSGEGEVENS

Persoonsgegevens en Verwijzingsgegevens

In het (decentrale) Incidentenregister van elk van de Verwerkingsverantwoordelijken en in het Centraal Incidentenregister worden de volgende gegevens vastgelegd:

- Persoonsgegevens van degenen die bij het Incident betrokken zijn, zoals naam, adres, woonplaats, telefoon, email (NAWTE)-gegevens, geboortedatum, nummer KvK.
- Strafrechtelijke persoonsgegevens indien de beschrijving van het gedrag van de Kaartgebruiker kwalificeert als Gedragingen. Strafrechtelijke persoonsgegevens zijn in dit verband persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. Hieronder vallen ook mogelijk gegronde verdenkingen. Dit wil zeggen dat er in de beschrijving van het Incident concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Daarnaast wordt er in dit kader verstaan: veiligheidsmaatregelen die verband houden met persoonsgegevens die te maken hebben met een door de rechter opgelegd verbod vanwege onrechtmatig of hinderlijk gedrag[13].
- Op het Incident betrekking hebbende gegevensdragers, zoals foto's, geluidsdragers en camerabeelden[14].
- Kenmerken van het Incident en de redenen voor opvoer van de melding.
- Handelingen die naar aanleiding van het Incident hebben plaatsgevonden.
- Maatregelen die naar aanleiding van het Incident zijn genomen.
- Indicatie of opname in het Centraal Incidentenregister Gatekeeper heeft plaatsgevonden.
- Naam van de Deelnemer.
- Naam van de Geautoriseerd functionaris die de melding heeft opgevoerd.
- De invoerdatum, de einddatum en bij eventuele mutaties: de datum van de mutatie en de naam van de Geautoriseerde Functionaris die de mutatie heeft doorgevoerd.
- de uitkomst van een eventuele bevraging.
- Indien van toepassing: aanhangig zijn van een eventuele bezwaar- of beroepsprocedure.
- Indien van toepassing: de uitkomst van een eventuele bezwaar- of beroepsprocedure.

De vastgelegde gegevens kunnen per Incident verschillen. Indien de Deelnemer besluit deze gegevens te delen met het Centraal Incidentenregister Gatekeeper worden deze gegevens hierna aangeduid als: **Verwijzingsgegevens**.

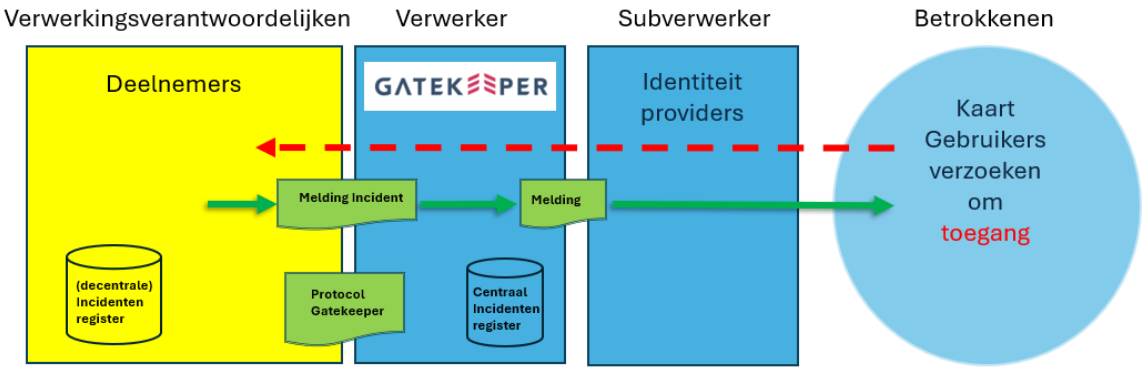
---

[13] https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#strafrechtelijke-gegevens

[14] Voor zover de beelden kwalificeren als het verwerken van bijzondere persoonsgegevens, vindt in overeenstemming met artikel 23 sub c UAVG plaats indien dit noodzakelijk is in aanvulling op de verwerking van strafrechtelijke persoonsgegevens voor de doeleinden waarvoor deze gegevens worden verwerkt of voor zover dit noodzakelijk is op grond van een wettelijke verplichting of de wetgeving (waaronder de AVG en UAVG) hierin voorziet. In zaken waarbij gebruik wordt gemaakt van een (drugs)uithaler, kan op een camerabeeld zijn vastgelegd wie zich bij containers bevond. Dit beeld vormt bewijs en is een belangrijk element in de vastlegging van het Incident.

3. AVG ROLLEN

Verwerkingsverantwoordelijken en (sub) verwerkers



Verwerkingsverantwoordelijken

De Deelnemers kwalificeren als *verwerkingsverantwoordelijken* omdat zij de doeleinden en de middelen bepalen waarmee de persoonsgegevens worden verwerkt in hun decentrale Incidentenregister en in het Centrale Incidentenregister Gatekeeper, namelijk het bestrijden van fraude en criminaliteit bij de Deelnemers, en het voorkomen van daaruit voortvloeiende corruptie, het beschermen van de veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de Deelnemers, het voorkomen van (excessief) geweld in de publieke ruimtes, en het voorkomen van economische- en imagoschade van de getroffen bedrijven. Verder bepalen de Deelnemers elk om, als middel om het doel te bereiken, gebruik te maken van het Centraal Incidentenregister Gatekeeper dat wordt beheerd door Stichting Gatekeeper. Alle verwerkingen worden verricht in het kader van toegangsmanagement dat onderdeel is van het beveiligings- en veiligheidsbeleid van de Deelnemers. Als een Incident zich voordoet, neemt de Deelnemer van die betreffende Hoog risico faciliteit de (Strafrechtelijke) Persoonsgegevens van de Kaartgebruiker op in zijn eigen Incidentenregister[15]. Verwacht de Deelnemer dat het geregistreerde gedrag zal kwalificeren als Gedragingen, dan deelt hij de Verwijzingsgegevens met het Centraal Incidentenregister Gatekeeper.

Verwerker

Stichting Gatekeeper kwalificeert als *verwerker* omdat zij deze Persoonsgegevens ten behoeve van de Verwerkingsverantwoordelijke Deelnemers verwerkt, op grond van artikel 28 AVG, de verwerkingsovereenkomst tussen elke Deelnemer (als Verwerkingsverantwoordelijke) en Stichting Gatekeeper. De voorwaarden waaronder de verschillende Deelnemers (Strafrechtelijke) Persoonsgegevens delen, zijn beschreven in dit protocol en liggen vast in de vergunning van de Autoriteit Persoonsgegevens. Wanneer zich een incident voordoet waarvan het gedrag van een Kaartgebruiker kwalificeert als Gedragingen, schakelt de Deelnemer Stichting Gatekeeper in als Verwerker. Stichting Gatekeeper verwerkt de Persoonsgegevens in het Centraal Incidentenregister, conform de instructies beschreven in de Verwerkersovereenkomst tussen elke Deelnemer met Stichting Gatekeeper.

[15] Conform artikel 10 AVG jo 33 lid 2 UAVG.

Sub verwerkers

Stichting Gatekeeper schakelt een of meerdere Identiteitsproviders in om ten behoeve van de Verwerkingsverantwoordelijken in het toegangsmanagementsysteem van de betreffende Deelnemer(s) het attribuut 'Gatekeeper' tijdelijk aan of uit te zetten. Deze Identiteitsproviders kwalificeren als sub verwerkers. Er is een (sub)verwerkersovereenkomst conform artikel 28 AVG tussen Stichting Gatekeeper en elke Identiteitsprovider. Identiteitsproviders verwerken de Persoonsgegevens in de toegangsmanagementsystemen, conform de instructies beschreven in de Verwerkersovereenkomst tussen Stichting Gatekeeper en elke Identiteitsprovider.

4. VERWERKINGEN EN DELEN VAN PERSOONSGEGEVENS

Het verwerken van Strafrechtelijke Persoonsgegevens is op grond van artikel 10 AVG (gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten) verboden, tenzij er sprake is van een uitzondering en mits een van de zes rechtsgrondslagen van artikel 6 AVG van toepassing is. De verwerkingen en uitzonderingen worden in dit hoofdstuk 4 beschreven. De rechtsgrondslagen van artikel 6 AVG worden in hoofdstuk 6 beschreven.

(1) Verwerkingen in het (decentrale) Incidentenregister bij de Deelnemers

Zoals gezegd kwalificeren Deelnemers als Verwerkingsverantwoordelijken. Deelnemers leggen beschrijvingen van Incidenten vast in het decentrale Incidentenregister van de betreffende Deelnemer. De uitzonderingsgrond op het verbod van het verwerken van Strafrechtelijke Persoonsgegevens van artikel 10 AVG (gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten) is de lidstaatrechtelijke bepalingen van artikel 33 lid 2 van de Uitvoeringswet AVG.

Alleen nadat is vastgesteld dat gedrag van een Kaartgebruiker kwalificeert als Gedragingen, mogen Deelnemers de Persoonsgegevens van die Kaartgebruiker uitwisselen met het Centraal Incidentenregister Gatekeeper en met andere Deelnemers. Dit gebeurt op grond van de vergunning van de Autoriteit Persoonsgegevens. De uitzonderingsgronden op het verbod voor het uitwisselen van de Verwijzingsgegevens van artikel 10 AVG zijn artikel 33 lid 4 sub c en lid 5 (vergunning AP) Uitvoeringswet AVG.

De Deelnemers blijven de mogelijkheid houden om voor hun eigen Faciliteiten hun eigen maatregelen te nemen op grond van de uitzondering van artikel 33 lid 2 Uitvoeringswet AVG.

In incidentele gevallen kan de politie (op grond van art 19 Wet Politiegegevens) of het Openbaar Ministerie (op grond van artikel 39f Wet justitiële en strafvorderlijke gegevens) aan Deelnemers informatie verstrekken. De uitzonderingsgrond op het verbod van artikel 10 AVG over het verwerken van strafrechtelijke persoonsgegevens door Deelnemers is in dit geval artikel 33 lid 1 sub a Uitvoeringswet AVG (‘*verkregen krachtens de Wet Politiegegevens of de Wet justitiële en strafvorderlijke gegevens*’).

(2) Verwerkingen in het Centraal Incidentenregister Gatekeeper

In het Centraal Incidentenregister Gatekeeper worden (Strafrechtelijke) Persoonsgegevens opgenomen. Het gaat om de Verwijzingsgegevens, afkomstig van de betreffende Deelnemers die gebruik maken van het Centraal Incidentenregister Gatekeeper dat wordt beheerd door Stichting Gatekeeper. Stichting Gatekeeper kwalificeert als *verwerker* omdat zij deze Persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke Deelnemers verwerkt, op grond van artikel 28 AVG, de verwerkingsovereenkomst tussen de Deelnemers en Stichting Gatekeeper.

In incidentele gevallen kan de politie (op grond van art 19 Wet Politiegegevens) of het Openbaar Ministerie (op grond van artikel 39f Wet justitiële en strafvorderlijke gegevens) aan Stichting Gatekeeper informatie verstrekken. De uitzonderingsgrond op het verbod van artikel 10 AVG over het verwerken van strafrechtelijke persoonsgegevens is in dit geval artikel 33 lid 1 sub a Uitvoeringswet AVG (‘*verkregen krachtens de Wet Politiegegevens of*

de Wet justitiële en strafvorderlijke gegevens') en artikel 33 lid 4 sub c en lid 5 (vergunning Autoriteit Persoonsgegevens) UAVG.

(3) Beperkt Persoonsgegevens delen met andere Deelnemers

Stichting Gatekeeper zal de Verwijzingsgegevens direct raadplegen. De Deelnemers krijgen, via het toegangsmanagementsysteem van de betreffende Identiteitsprovider, slechts te zien *dat* een Kaartgebruiker geen toegang krijgt (met daarbij een telefoonnummer voor informatie). Deze risico beperkende Maatregel houdt verband met data minimalisatie.

Daarnaast deelt Stichting Gatekeeper in beginsel met de betreffende Deelnemer die de initiële melding heeft gedaan alleen *dat* een Maatregel is opgelegd, zonder nadere toelichting. Op deze wijze zijn gegevens uit het Centraal Incidentenregister Gatekeeper op een zorgvuldige, beperkte en gecontroleerde wijze beschikbaar voor de Deelnemers. Ook de melding aan de poort van een Deelnemer dat tijdelijk de toegang is beperkt voor een Kaartgebruiker wordt beschouwd als het verwerken van (Strafrechtelijke) Persoonsgegevens. Deze handeling is toegestaan op basis van dit protocol en de verstrekte vergunning van de Autoriteit Persoonsgegevens.

Slechts wanneer dit nodig is voor het onderzoek rond een klacht, geschil of beroep, zal Stichting Gatekeeper besluiten om een Geautoriseerde functionaris van (in eerste instantie) de meldende Deelnemer en eventueel later ook andere Geautoriseerde functionarissen of leden van de geschillen of beroepscommissie toegang te verlenen tot (in eerste instantie) het betreffende dossier en eventueel later ook andere dossiers, inclusief namen. Terughoudendheid is hierbij geboden. Toegang wordt verleend wanneer er sprake is van een van onderstaande voorwaarden:

1. het betreft een Geautoriseerde functionaris van een of meer Deelnemers, die kan helpen om meer informatie in te winnen;
2. het betreft een Geautoriseerde functionaris die, gezien zijn ervaring en relevantie met het betreffende dossier, advies kan geven over een op te leggen Maatregel;
3. het betreft een Geautoriseerde functionaris die kan helpen bij het onderzoek van Incidenten van het betreffende dossier;
4. het betreft een Geautoriseerde functionaris die kan helpen bij het beoordelen van mogelijke Maatregelen.

De uitzonderingsgronden op het verbod voor het delen van Strafrechtelijke Persoonsgegevens van artikel 10 AVG zijn artikel 33 lid 1 sub a Uitvoeringswet AVG en artikel 33 lid 2 en lid 4 sub b en sub c en lid 5 (vergunning Autoriteit Persoonsgegevens) Uitvoeringswet AVG.

Wanneer een Geautoriseerde functionaris Stichting Gatekeeper verzoekt om informatie te delen die de Geautoriseerde functionaris nodig heeft voor trendanalyses en het ontwikkelen van fraude en criminaliteit preventie strategieën van de betreffende Deelnemer zal Stichting Gatekeeper dit delen, op een zodanig geaggregeerd niveau dat personen niet te identificeren zijn.

(4) (sub)Verwerkingen door Identiteitsproviders

Verschillende Identiteitsproviders werken met toegangsmanagementsystemen die Kaartgebruikers alleen toegang verlenen tot bepaalde faciliteiten als zij beschikken over de vereiste attributen, waaronder het attribuut 'Gatekeeper'. Indien Stichting Gatekeeper het voorstel voor een Maatregel van een Deelnemer proportioneel acht, zal zij de

Identiteitsproviders (als sub verwerkers) instrueren om in hun systemen het attribuut ‘Gatekeeper’ tijdelijk uit te zetten. Wanneer het attribuut ‘Gatekeeper’ uitstaat, krijgt de Kaartgebruiker geen automatische toegang tot de Hoog risico faciliteit[16]. Hiermee worden gegevens uit het Centraal Incidentenregister Gatekeeper op een zorgvuldige, beperkte en gecontroleerde wijze beschikbaar voor de Deelnemers en de Identiteitsproviders. De relevante artikelen hierbij zijn artikel 28 AVG, de (sub)verwerkingsovereenkomst tussen Stichting Gatekeeper en Identiteitsproviders, en de uitzonderingsgronden op artikel 10 AVG: de lidstaatrechtelijke bepalingen van artikel 33 lid 1 sub a Uitvoeringswet AVG en artikel 33 lid 2 en lid 4 sub b en sub c en lid 5 (vergunning Autoriteit Persoonsgegevens) Uitvoeringswet AVG. De Identiteitsproviders dienen te voldoen aan de AVG en toepasselijke technische en organisatorische beveiligingsmaatregelen te nemen.

[16] De Kaartgebruiker kan vervolgens nog wel om toegang verzoeken bij de portiersloge met als mogelijk gevolg dat de Kaartgebruiker toch toegang krijgt.

5. BEGINSELEN INZAKE VERWERKING VAN PERSOONSGEGEVENS (Art 5 AVG)

Persoonsgegevens in het Incidentenregister en in het Centraal Incidentenregister dienen te worden verwerkt op een wijze die ten aanzien van de Kaartgebruiker rechtmatig, behoorlijk en transparant is.

Rechtmatigheid

In hoofdstuk 6 wordt dieper ingegaan op de rechtmatigheid van de verwerkingen in het kader van artikel 6 AVG. Hier beschrijven we de rechtmatigheid aan de hand van artikel 5 AVG: beginselen inzake de verwerking van Persoonsgegevens. Omdat fraude en criminaliteit zich niet beperken tot de faciliteiten van de Deelnemers en omdat het effect diep doorwerkt in de maatschappij is het instellen van een Afsprakenstelsel zoals beschreven in dit protocol een rechtmatig belang.

Behoorlijk

De behoorlijkheid is gewaarborgd in de statuten van Stichting Gatekeeper en het reglement voor de directie van Gatekeeper. De raad van toezicht, bestaande uit leden met ruime ervaring in de logistieke sector, controleert de directie van Stichting Gatekeeper. Daarnaast adviseert, ondersteunt en controleert een raad van advies de directie van Stichting Gatekeeper. De raad van advies bestaat uit leden uit publieke organisaties. Zie ook alinea ‘Regels voor toezicht, audit, evaluatie en wijzigingen’.

Transparant

Deelnemers informeren hun Kaartgebruikers via openbare privacy statements op hun websites. Daarnaast zorgt de website www.stichtinggatekeeper.nl voor transparantie omdat daar relevante documenten worden gepubliceerd. Denk aan informatie over Gatekeeper, het overzicht van de Deelnemers, de statuten, het directiereglement en reglement Raad van Toezicht Gatekeeper, het privacy statement en de Integriteitsovereenkomst. Buitenlandse Kaartgebruikers komen uit EU-landen en hebben dezelfde rechten onder de AVG. Stichting Gatekeeper zorgt ervoor dat buitenlandse Kaartgebruikers worden geïnformeerd in de gebruikelijke talen. Naast Nederlands zijn dat Engels, Duits, Frans, Spaans, Pools, Bulgaars en Roemeens. Buitenlandse Kaartgebruikers werken meestal voor werkgevers en die werkgevers zullen, voordat hun werknemers toegang krijgen, eerst een Integriteitsovereenkomst met Stichting Gatekeeper ondertekenen. Op die grond zal Stichting Gatekeeper de werkgever beperkt informeren als een Maatregel is genomen, zonder verdere details over het Incident. Stichting Gatekeeper zal Persoonsgegevens die in het Gatekeeper Centraal Incidentenregister worden verwerkt niet delen met werkgevers buiten Nederland.

Stichting Gatekeeper zal de Kaartgebruiker per email een bevestiging van opname in het Centraal Incidentenregister Gatekeeper sturen. De inhoud van deze e-mail omvat de volgende informatie: de datum, de identiteitsgegevens van de Kaartgebruiker, de reden voor registratie in het Centraal Incidentenregister Gatekeeper, de termijn van opname in het Centraal Incidentenregister Gatekeeper, een (web)adres waar de Kaartgebruiker kan raadplegen welke organisaties (de Deelnemers) gebruik maken van Centraal Incidentenregister Gatekeeper, gegevens van de Deelnemer die de melding heeft ingevoerd, het recht om bezwaar te maken tegen de opname in het Centraal Incidentenregister Gatekeeper, uitleg over de klacht-, bezwaar- en beroep procedure, het

adres van Stichting Gatekeeper waar de klacht of het bezwaarschrift of beroepschrift aan gericht mag worden.

Doelbinding

Het Incidentenregister en het Centraal Incidentenregister richten zich op het herkennen, voorkomen, onderzoeken en bestrijden van crimineel gedrag en fraude die schadelijk kunnen zijn voor de economische eenheid waar de Deelnemer deel van uitmaakt, de Deelnemer zelf, zijn leveranciers (onder wie vervoerders), klanten en medewerkers. De Persoonsgegevens in het Incidentenregister en in het Centraal Incidentenregister worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, namelijk het bestrijden van fraude en criminaliteit bij de Deelnemers, en het voorkomen van daaruit voortvloeiende corruptie, het beschermen van de veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de Deelnemers, het voorkomen van (excessief) geweld in de publieke ruimtes, en het voorkomen van economische- en imagoschade van de getroffen bedrijven. Verdere verwerking zal alleen plaatsvinden indien dit met deze doeleinden verenigbaar is. De toegang tot Verwijzingsgegevens die opgeslagen zijn in het Centraal Incidentenregister Gatekeeper is in beginsel beperkt tot de medewerkers van Stichting Gatekeeper. Een uitzondering zal zijn dat een Geautoriseerde functionaris van een Deelnemer toegang krijgt tot een bepaald dossier in het kader van een onderzoek, het beoordelen van mogelijke Maatregelen, trendanalyses en het ontwikkelen van fraude en criminaliteit preventie strategieën.

Minimale gegevensverwerking

Persoonsgegevens in het Incidentenregister en in het Centraal Incidentenregister worden niet langer dan nodig en zodanig verwerkt dat zij toereikend en ter zake dienend zijn. Dit betreft gedrag van een Kaartgebruiker dat kwalificeert als Gedragingen. Zie verder alinea ’Criteria rond het opleggen van een Maatregel’. De partijen delen alleen de noodzakelijke informatie.

Juistheid

De Persoonsgegevens in het Incidentenregister en in het Centraal Incidentenregister dienen correct en actueel te zijn. Indien blijkt dat Persoonsgegevens onjuist zijn, worden deze onverwijld gewist of gerectificeerd.

Opslagbeperking

Persoonsgegevens worden niet langer dan nodig bewaard. De Persoonsgegevens in het Centraal Incidentenregister worden zodanig bewaard dat de Kaartgebruikers alleen te identificeren zijn voor de duur van de doeleinden waarvoor de gegevens noodzakelijk zijn. Als een registratie onterecht is, worden de Persoonsgegevens direct verwijderd. Als een Maatregel is opgelegd, worden de Persoonsgegevens vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse taak van Stichting Gatekeeper. De bewaartermijn is maximaal 5 jaar na de datum van eerste verwerking, tenzij er een nieuwe aanleiding is die de registratie rechtvaardigt.

De termijn van 5 jaar zorgt ervoor dat het dossier in geval van recidive te raadplegen is. In geval van recidive kan de Kaartgebruiker, in plaats van voor 3 maanden, de toegang voor een periode van 1 jaar worden beperkt. Recidive is een serieus probleem: In 2019 heeft bijna 68% van de strafzaken binnen het volwassenen strafrecht die leidde tot een veroordeling van de rechter of een afdoening door het OM, betrekking op daders die al eerder een veroordeling van de rechter of een afdoening van het OM op hun naam hebben

staan[17]. Naar verwachting zal recidive 5 jaar na de beperking van toegang niet vaak voorkomen; langer bewaren van de gegevens is niet noodzakelijk. Voor deze bewaartermijn is ook gekozen omdat het gaat om gedrag dat kwalificeert als Gedragingen. De Deelnemers en Stichting Gatekeeper moeten er rekening mee houden dat zij de gegevens nodig kunnen hebben voor de instelling, uitoefening of onderbouwing van een rechtsvordering, conform artikel 32 onder (d) Uitvoeringswet AVG of onder artikel 3:310 lid 1 BW. Beide hebben een termijn van 5 jaar. Ten slotte is aansluiting gezocht bij de terugkijktermijn die Justis[18] hanteert voor Verklaringen Omtrent Gedrag in de categorie 'Wegvervoerondernemer goederenvervoer'. Deze termijn is ook 5 jaar. De Deelnemers en Stichting Gatekeeper nemen verder passende technische en organisatorische maatregelen om de rechten en vrijheden van de Kaartgebruiker (waaronder de Strafrechtelijke Persoonsgegevens) te beschermen tijdens de bewaartermijn, conform artikel 32-34 AVG.

Integriteit en vertrouwelijkheid

Conform artikel 32 AVG nemen Deelnemers, Stichting Gatekeeper en de Identiteitsproviders passende technische en organisatorische maatregelen om de beveiliging van Persoonsgegevens te waarborgen. De Persoonsgegevens dienen onder meer beschermd te zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De Persoonsgegevens die in het kader van dit protocol worden verwerkt en opgenomen in het Incidentenregister en het Centraal Incidentenregister Gatekeeper dienen strikt vertrouwelijk te worden behandeld. Iedere Deelnemer treft passende voorzieningen die waarborgen dat de Geautoriseerde functionaris onder een geheimhoudingsplicht valt. Geautoriseerde functionarissen zijn geïnformeerd over de werking van het Afsprakenstelsel. Zij worden er nadrukkelijk op gewezen dat het gebruik van het Afsprakenstelsel uitsluitend is toegestaan binnen de regels van dit protocol en de binnen de geldende interne procedures en voorschriften. Iedere Deelnemer voldoet aan de verplichtingen aangaande het voorkomen van datalekken overeenkomstig artikel 33 AVG en artikel 34 AVG en implementeert een procedure die hiervoor zorgdraagt.

Verantwoordingsplicht

De Deelnemer neemt de verwerking van Persoonsgegevens in het kader van dit protocol op als een aparte activiteit in zijn register van verwerkingsactiviteiten. Daarnaast houdt de Deelnemer bij welke Persoonsgegevens hij heeft gedeeld met het Centraal Incidentenregister. Deelnemers en Stichting Gatekeeper registreren wie gemeld heeft, waar de melding vandaan komt en wanneer de melding is gedaan. De directie van Stichting Gatekeeper dient de overwegingen, de beoordeling en de Maatregel te documenteren en veilig op te slaan. Daarnaast houdt Stichting Gatekeeper als Verwerker bij welke Persoonsgegevens zij heeft gedeeld met de Deelnemer(s).

[17] Wetenschappelijk Onderzoek en Datacentrum Rijksoverheid (WODC) Cahier 2021-21 rapport 'Recidive onder justitiabelen in Nederland, Verslag over de periode 2008-2020', Verweij e.a., p. 12.

[18] Justis is onderdeel van het Ministerie van Justitie en Veiligheid. https://www.justis.nl/producten/verklaring-omtrent-het-gedrag-vog/beoordeling-besluit-en-bezwaar/terugkijktermijnen#:~:text=De%20terugkijktermijn%20voor%20een%20VOG%20P%20is%2010%20jaar%20voor,om%20functies%20met%20hoge%20integriteitseisen.

6. RECHTMATIGHEID VAN DE VERWERKINGEN (Art 6 AVG)

De verwerking van Strafrechtelijke Persoonsgegevens is op grond van artikel 10 AVG in beginsel verboden, tenzij sprake is van een uitzondering, zoals beschreven in hoofdstuk 4. Binnen het Afsprakenstelsel Gatekeeper wordt een beroep gedaan op artikel 33 lid 4 sub c UAVG, dat verwerking ten behoeve van derden toestaat indien daarvoor een vergunning is verleend door de Autoriteit Persoonsgegevens. Deze vergunning mag worden afgegeven indien de verwerking noodzakelijk is wegens een zwaarwegend belang van derden en mits de verwerking gepaard gaat met passende waarborgen (artikel 33 lid 5 UAVG). Daarnaast moet de verwerking op grond van artikel 6 AVG ook een rechtmatige grondslag hebben. Binnen dit kader wordt een beroep gedaan op het gerechtvaardigd belang van de Verwerkingsverantwoordelijke Deelnemers (artikel 6 lid 1 sub f AVG). Om dit aan te tonen wordt de driestappentoets toegepast. Daarin komen ook de elementen noodzakelijkheid, zwaarwegend belang van derden en passende waarborgen terug.

1. Belangen van betrokken Kaartgebruikers

Betrokken Kaartgebruikers hebben het recht op bescherming van hun persoonlijke levenssfeer, waaronder hun strafrechtelijk verleden. Zij hebben recht op rehabilitatie en een nieuw begin, zonder blijvende stigmatisering of uitsluiting.

Onnodige of onevenredige verwerking van strafrechtelijke persoonsgegevens zou de ontwikkeling van identiteit en reputatie van de Kaartgebruiker kunnen beperken, en zou risico's met zich mee kunnen brengen op misbruik of datalekken, met mogelijke reputatieschade, belemmeringen op de arbeidsmarkt en sociale uitsluiting als gevolg. De AVG, het EVRM en het Nederlands strafrecht beschermen deze belangen.

2. Belangen van afzonderlijke Deelnemers

Tegenover deze belangen staat het recht van elke afzonderlijke Deelnemer die wordt geconfronteerd met georganiseerde en herhaalde vormen van fraude, criminaliteit en (excessief geweld) op haar faciliteiten. Hieruit vloeit corruptie voort, en onveilige situaties voor personen die werkzaam zijn op of zich bevinden binnen hoog risico faciliteiten van elke Deelnemer. Dit kan ook zorgen voor imagoschade en economische schade voor elke afzonderlijke Deelnemer.

Preventie van fraude, criminaliteit en misbruik van diensten wordt aangemerkt als een gerechtvaardigd belang[19] en het tegengaan van fraude geldt als een zwaarwegend belang voor een bedrijf of onderneming[20]. Zo heeft elke afzonderlijke Deelnemer een gerechtvaardigd en zwaarwegend algemeen belang om haar medewerkers, klanten, eigendommen en reputatie te beschermen tegen schade door fraude, geweld of criminele inmenging. Zij dragen een zorgplicht voor een veilige werkplek en zijn bovendien verantwoordelijk voor de toegang tot gevoelige of risicovolle locaties. Een van de mogelijke maatregelen om aan deze zorgplicht te voldoen, is de toegang tot Hoog risico faciliteiten van Deelnemers tijdelijk te beperken voor Kaartgebruikers die een Gedraging vertonen. De

[19] WP 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46EC, WP 217. Hierin is opgenomen dat onder meer preventie van fraude, criminaliteit en misbruik van diensten wordt aangemerkt als een gerechtvaardigd belang.
[20] Kamerstukken II 2017-18, 34851, nr. 7 Nota naar aanleiding van het verslag, p. 55.

aanwezigheid van personen die ongewenst gedrag vertonen kan een direct risico vormen dat niet altijd op basis van eigen waarneming of openbare bronnen kan worden ingeschat. Zonder toegang tot relevante informatie van andere Deelnemers ontbreekt het hen aan een reële mogelijkheid om preventieve maatregelen te nemen.

Het feit dat iemand geregistreerd staat in het Centraal Incidentenregister Gatekeeper, wordt gedeeld met de andere Deelnemers om benadeling van betreffende Deelnemers en de personen die zich op de faciliteiten van de Deelnemers bevinden helpen te voorkomen en bij te dragen aan een veiligere werkomgeving. Dit is belangrijk voor elke afzonderlijke Deelnemer.

Aanvullende maatregel om ongewenst gedrag van Kaartgebruikers te verminderen

Gelet op de toenemende mate waarin ongewenst gedrag plaatsvindt en de veiligheidsrisico's en financiële schade daarvan voor Deelnemers, vormt dit ongewenst gedrag een groot probleem dat met de huidige middelen onvoldoende bestreden kan worden. Het Centraal Incidentenregister Gatekeeper dient dan ook als aanvullende maatregel om ongewenst gedrag van Kaartgebruikers te verminderen. Registratie in het Centraal Incidentenregister Gatekeeper vindt pas plaats wanneer Kaartgebruikers ongewenst gedrag vertonen dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen.

De Deelnemers hebben zich rekenschap gegeven van de noodzakelijke belangenafweging tussen het belang van de Deelnemers in de logistieke sector en de inbreuk op de persoonlijke levenssfeer en de andere rechten en vrijheden van de Kaartgebruiker bij diens registratie in het Centraal Incidentenregister Gatekeeper. Dit blijkt uit de invulling van de begrippen proportionaliteit en subsidiariteit.

Noodzakelijkheid

De verwerking van Persoonsgegevens en het opleggen van een Maatregel moet noodzakelijk zijn om het belangen van de afzonderlijke Deelnemer te realiseren bij het bestrijden van fraude en criminaliteit, het voorkomen van daaruit voortvloeiende corruptie, het beschermen van de veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de Deelnemers, het voorkomen van (excessief) geweld in de publieke ruimtes, en het tegengaan van economische- en imagoschade van de getroffen Deelnemer.

Deelnemers verwachten met het Centraal Incidentenregister Gatekeeper fraude en criminaliteit op hun faciliteiten te kunnen bestrijden, daaruit voortvloeiende corruptie te voorkomen, veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de afzonderlijke Deelnemer beter te beschermen, (excessief) geweld in de publieke ruimtes te kunnen voorkomen en economische- en imagoschade van de getroffen bedrijven tegen te kunnen gaan. Tevens verwachten Deelnemers dat er van het Centraal Incidentenregister Gatekeeper een preventieve werking uitgaat. Het doel van de verwerking is dan ook meervoudig:

- Het bestrijden van georganiseerde criminaliteit en fraude binnen de aangesloten organisaties
- Het voorkomen van corruptie en het ondermijnen van veiligheid
- Het beschermen van personen die werkzaam zijn op of zich bevinden binnen hoog risico faciliteiten van afzonderlijke Deelnemers

- Het voorkomen van imagoschade en economische schade, zowel voor afzonderlijke Deelnemers als voor de gezamenlijke Deelnemers

3. Gezamenlijk belang van Deelnemers

De belangen van de afzonderlijke Deelnemers gelden ook voor de Deelnemers gezamenlijk. Er bestaat er een zwaarwegend algemeen belang bij collectieve samenwerking en informatie-uitwisseling. Deze belangen overstijgen het belang van een afzonderlijke Deelnemer. Het algemene belang krijgt daarbij een extra dimensie door de verwevenheid van de Deelnemers in een logistiek systeem waarin veiligheid en vertrouwen tussen partijen essentieel zijn. Deze collectieve kwetsbaarheid vereist samenwerking en informatie-uitwisseling om dreigingen effectief het hoofd te bieden want frauduleuze en criminele gedragingen doen zich vaak keten-breed voor, waarbij dezelfde personen zich bij meerdere Deelnemers aandienen.

Fraude en criminaliteit op deze faciliteiten hebben vaak gevolgen die verder reiken dan de individuele Deelnemer. Meerdere Deelnemers worden regelmatig gelijktijdig of opeenvolgend geraakt, waardoor het noodzakelijk is dat informatie over Gedragingen tijdig gedeeld wordt want criminelen proberen het vaak opnieuw bij een andere Deelnemer. De verwerking van Strafrechtelijke Persoonsgegevens en de onderlinge uitwisseling daarvan zijn daarbij essentiële handelingen voor de Verwerkingsverantwoordelijke Deelnemers, zodat zij Kaartgebruikers die gedrag vertonen dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen, de toegang tot Hoog risico faciliteiten kunnen beperken.

Het delen van signalen is daarom essentieel om herhaald slachtofferschap te voorkomen en gezamenlijk op te treden tegen structurele dreigingen. Door dit gezamenlijke stelsel ontstaat een versterkt beveiligingsniveau dat individuele maatregelen overstijgt.

Zonder tijdige signalering kan een aaneenschakeling van samenhangende of gelijksoortige fraude en criminaliteit plaatsvinden bij andere Deelnemers, met aanzienlijke nadelige gevolgen voor (lucht)havenbedrijven, distributie- en transportbedrijven en de veiligheid van hun medewerkers. Het delen van informatie en het tijdig waarschuwen binnen het Afsprakenstelsel is daarom onmisbaar. Bovendien rust op Deelnemers de wettelijke en maatschappelijke zorgplicht om de veiligheid van hun medewerkers te waarborgen en om fraude en criminaliteit actief tegen te gaan.

Driestappentoets

1. Doeleindtoets: Is er sprake van een gerechtvaardigd belang?

Ja. De afzonderlijke Deelnemers en de Deelnemers gezamenlijk hebben een aantoonbaar gerechtvaardigd en zwaarwegend algemeen belang bij het verwerken van strafrechtelijke persoonsgegevens:

- Ter bestrijding van fraude en criminaliteit bij de Deelnemers.
- Voor het beschermen van de veiligheid van personen op Hoog risico faciliteiten van de Deelnemers.
- Voor het voorkomen van (excessief) geweld in publieke ruimtes en corruptie.
- Ter voorkoming van economische of imagoschade van de Deelnemers.

- Om een aaneenschakeling van samenhangende of gelijksoortige fraude en criminaliteit bij andere Deelnemers te voorkomen.

Deze belangen worden ondersteund door de AVG (Overweging 47), het WP 29-advies WP217[21], en de wetsgeschiedenis van de UAVG[22], waarin fraude expliciet wordt erkend als een zwaarwegend belang. Fraude en criminaliteit zijn ernstige zaken die op diverse plaatsen in het Wetboek van Strafrecht strafbaar zijn gesteld, met mogelijk aanzienlijke sancties. Het effect van de fraude en criminaliteit is voelbaar bij elke Deelnemer afzonderlijk, bij de Deelnemers gezamenlijk, binnen de gehele logistieke keten en zelfs tot diep in de maatschappij.

2. Noodzakelijkheidstoets: Is de verwerking noodzakelijk voor dit doel?

Ja. De verwerking en onderlinge uitwisseling van persoonsgegevens zijn noodzakelijk omdat:

- Criminelen zich herhaaldelijk of bij de afzonderlijke Deelnemer en bij verschillende Deelnemers kunnen aandienen.
- Incidenten vaak niet geïsoleerd zijn en zich in ketens of patronen voordoen.
- Uitsluitend melding bij opsporingsdiensten onvoldoende is voor preventie bij andere Deelnemers.
- Deelnemers een zorgplicht hebben richting hun medewerkers en derden.
- Er is geen minder ingrijpende manier om het doel te bereiken.

Zonder deze informatie-uitwisseling lopen Deelnemers verhoogde risico's en zou het beveiligingsniveau op de faciliteiten van de Deelnemers. De proportionaliteit wordt geborgd door beperkingen in gegevensverwerking, uitgebreide waarborgen, en de verplichting om te handelen conform dit protocol en een door de Autoriteit Persoonsgegevens verleende vergunning.

4. Belangenafweging: Wegen de belangen van de afzonderlijke en gezamenlijke Deelnemers zwaarder dan de privacyrechten van betrokken Kaartgebruikers?

De verwerking van strafrechtelijke persoonsgegevens raakt de persoonlijke levenssfeer van de Kaartgebruiker en vereist daarom bijzondere terughoudendheid. Deelnemers onderkennen dat de registratie van betrokkene in het Centraal Incidentenregister Gatekeeper kan leiden tot nadelige gevolgen voor betrokkene, namelijk dat de strafrechtelijke persoonsgegevens, indien onzorgvuldig verwerkt, kunnen leiden tot stigmatisering en uitsluiting, bijvoorbeeld bij sollicitaties of werk. De Kaartgebruiker heeft er bovendien een belang bij om niet blijvend geconfronteerd te worden met fouten uit het verleden, in het licht van het fundamentele recht op rehabilitatie en een nieuw begin.

Deelnemers hebben echter voldoende waarborgen getroffen om dit risico zoveel mogelijk te beperken, door onder meer restricties aan te brengen voor wat betreft de registratie en

[21] WP 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46EC, WP 217. Hierin is opgenomen dat onder meer preventie van fraude, criminaliteit en misbruik van diensten wordt aangemerkt als een gerechtvaardigd belang.
[22] Kamerstukken II 2017-18, 34851, nr. 7 Nota naar aanleiding van het verslag, pagina 55. Hierin is opgenomen dat het tegengaan van fraude als een zwaarwegend belang voor een bedrijf of onderneming geldt.

de raadpleging van het Centraal Incidentenregister Gatekeeper. Registratie zal alleen plaatsvinden bij gedrag van een Kaartgebruiker dat bestaat uit zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen. Raadpleging van het Centraal Incidentenregister Gatekeeper is beperkt tot een melding dat de Kaartgebruiker geen toegang heeft, met slechts een telefoonnummer voor meer informatie.

Voorts hanteren de Deelnemers aan het Afsprakenstelsel Gatekeeper vooraf gecommuniceerde criteria over soorten ongewenst gedrag voor registratie in het Centraal Incidentenregister Gatekeeper. Die criteria zijn opgenomen in de integriteitsovereenkomst tussen de Deelnemers en de Kaartgebruiker:

2. Ik betreed de faciliteiten alleen op basis van een gerechtvaardigd en legaal doel;

3. Ik voer geen onrechtmatige handelingen uit en zal terstond melding maken zodra ik kennis neem van of betrokken dreig te raken bij fraude, criminele activiteiten of zaken die de veiligheid op de faciliteiten beïnvloeden;

4. Ik breng geen mensen of goederen op het terrein die niet op het terrein horen;

Verder maakt de afzonderlijke Deelnemer een afweging en vindt hoor en wederhoor plaats voordat een Kaartgebruiker wordt geregistreerd in het Centraal Incidentenregister Gatekeeper. Er is door klacht, bezwaar en beroepsprocedures voorzien in de mogelijkheid om in een individuele situatie van de criteria af te wijken in het voordeel van de Kaartgebruiker. In het protocol is neergelegd dat de gebruikelijke duur van de toegangsbeperkende maatregel drie maanden is (in uitzonderlijke gevallen te verlengen) en dat de gegevens niet langer dan 5 jaar worden bewaard, waarbij is aangesloten bij strafrechtelijke bewaartermijnen en dat de Deelnemers er rekening mee moeten houden dat zij de gegevens nodig kunnen hebben voor een rechtsvordering, conform artikel 32 onder (d) UAVG of onder artikel 3:310 lid 1 BW. Beide hebben een termijn van 5 jaar. De Deelnemers aan het Afsprakenstelsel Gatekeeper hebben afgewogen dat betrokken Kaartgebruikers niet langer dan noodzakelijk wordt geconfronteerd met in het verleden begane ongewenst gedrag. Voor wat betreft de beveiliging hebben de Deelnemers passende technische en organisatorische maatregelen getroffen, zo is de fysieke en digitale toegang tot het Centraal Incidentenregister Gatekeeper beperkt tot de daartoe geautoriseerde medewerkers. Daarnaast zijn deze geautoriseerde medewerkers verplicht tot geheimhouding van de gegevens.

De rechten van betrokkenen in de AVG voorzien in belangrijke corrigerende waarborgen tegen ongerechtvaardigde inbreuken op de persoonlijke levenssfeer van betrokkenen. Deelnemers vullen deze rechten in, zo is in het protocol de wettelijke informatieplicht uitgewerkt en wordt aan betrokkenen de mogelijkheid geboden om inzage van de verzamelde gegevens te verzoeken. Binnen de wettelijk vastgestelde termijn van vier weken wordt een volledig schriftelijk overzicht in begrijpelijke vorm verstrekt van de aard en omvang van de verzamelde gegevens van betrokkene en het gebruik dat ervan gemaakt wordt. Daarnaast kan een betrokkene verzoeken zijn gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze onjuist, onvolledig of niet ter zake dienend zijn, of in strijd met een wettelijk voorschrift worden verwerkt.

Als de verwerking en uitwisseling van Persoonsgegevens niet mogelijk zijn, krijgen criminelen vrij spel op de faciliteiten van de afzonderlijke Deelnemer of verplaatsen zij hun

activiteiten eenvoudig naar andere Deelnemers. Er is geen minder ingrijpende manier beschikbaar om hetzelfde beschermingsniveau te realiseren.

De belangen van Deelnemers en Kaartgebruikers raken beide fundamentele rechten en vrijheden. Binnen het Afsprakenstelsel Gatekeeper is echter voorzien in strikte waarborgen om het recht van Kaartgebruikers op eerlijke behandeling en privacy te beschermen:

- De verwerking vindt uitsluitend plaats bij een gerechtvaardigde aanleiding (concrete gedraging).
- Er zijn heldere criteria vooraf, en wanneer Deelnemers registratie overwegen zal er hoor en wederhoor plaatsvinden.
- Er is sprake van doelbinding, noodzakelijkheid en proportionaliteit, onder meer doordat Deelnemers verplicht zijn zich te houden aan dit protocol en aan de voorwaarden van de door de Autoriteit Persoonsgegevens verstrekte vergunning.
- Er is sprake van dataminimalisatie en de gegevens worden uitsluitend gedeeld binnen een gesloten, beveiligd stelsel met vergunning van de Autoriteit Persoonsgegevens.
- Kaartgebruikers behouden rechten op bezwaar, inzage en correctie, met extra rechtsbescherming via geschillenprocedures.
- Er wordt gewerkt met tijdslimieten en herbeoordelingsmomenten om blijvende stigmatisering te voorkomen.
- Er worden niet méér of te gevoelige persoonsgegevens verwerkt dan strikt noodzakelijk is, en er zijn diverse technische en organisatorische waarborgen doorgevoerd om te verzekeren dat de verwerking plaatsvindt op een manier die de privacy van de betrokken Kaartgebruikers niet onevenredig schaadt.

Gelet op de ernst, frequentie en maatschappelijke impact van de risico's die zonder verwerking onbestreden zouden blijven, en gezien de technische, organisatorische en juridische waarborgen die getroffen zijn, wegen de gerechtvaardigde belangen van elke Deelnemer afzonderlijk en de gerechtvaardigde belangen van de Deelnemers gezamenlijk zwaarder dan de inbreuk die de verwerking onder deze voorwaarden maakt op de rechten van Kaartgebruikers.

Conclusie driestappentoets

Hoewel Kaartgebruikers er belang bij hebben dat er geen inbreuk wordt gemaakt op hun persoonlijke levenssfeer om stigmatisering en uitsluiting te voorkomen, wegen de belangen van de Deelnemers bij het bestrijden van fraude en criminaliteit bij de Deelnemers, en het voorkomen van daaruit voortvloeiende corruptie, het beschermen van de veiligheid van de personen die zich bevinden op de Hoog risico faciliteiten van de Deelnemers, het voorkomen van (excessief) geweld in de publieke ruimtes, en het voorkomen van economische- en imagoschade van de getroffen bedrijven, onder de waarborgen beschreven in dit protocol, zwaarder dan de belangen van individuele Kaartgebruikers die gedrag vertonen dat aanleiding geeft tot gerechtvaardigde Maatregel binnen het Afsprakenstelsel Gatekeeper.

Uitkomst DPIA: beperkt rest risico

Omdat zij in bepaalde gevallen Strafrechtelijke Persoonsgegevens verwerken en delen, hebben de Deelnemers en Stichting Gatekeeper de verplichte Gegevensbeschermingseffectbeoordeling (GEB, meestal DPIA genoemd) uitgevoerd. Uit de

DPIA blijkt dat er geen hoog privacy risico resteert voor de Kaartgebruikers en dat met beheersmaatregelen het risico kan en zal worden beperkt. Daarom vragen Verwerkingsverantwoordelijken een model vergunning aan bij de AP.

Modelvergunning Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens heeft voor de verwerking van Strafrechtelijke Persoonsgegevens overeenkomstig dit model protocol aan de Deelnemer die hierom verzoekt een model vergunning verstrekt conform artikel 33 lid 5 Uitvoeringswet AVG.

Conclusie belangenafweging

Op grond van bovengenoemde overwegingen wordt geconcludeerd dat de Deelnemers bij de verwerking van Persoonsgegevens in het kader van dit protocol zich kunnen baseren op de grondslag van artikel 6 lid 1 sub f AVG, het gerechtvaardigd belang. De verwerkingen zijn noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de Verwerkingsverantwoordelijken (de Deelnemers) en de belangen of de grondrechten en de fundamentele vrijheden van de Kaartgebruikers wegen gezien de in dit protocol beschreven omstandigheden niet zwaarder dan de gerechtvaardigde belangen van de Deelnemers.

7. ANDERE REGELS VOOR DEELNEMERS EN STICHTING GATEKEEPER

Regels voor beoordeling van een melding

De Geautoriseerde functionaris van een Deelnemer beoordeelt het gemelde gedrag van Kaartgebruikers binnen hun eigen Hoog risico faciliteit aan de hand van dit protocol. Afhankelijk van de inhoud van de melding zal het gedrag kwalificeren als Gedragingen. Indien dat het geval is, is een Maatregel op zijn plaats zijn, anders niet. De meldende Deelnemer dient daarbij te beoordelen of het waargenomen gedrag kwalificeert als Gedragingen en of de op te leggen Maatregel effectief is op twee gebieden:

1. Verbetert de Maatregel de veiligheid op de Hoog risico faciliteiten van de Deelnemers?
2. Zal de Maatregel criminaliteit op de Hoog risico faciliteiten van Deelnemers redelijkerwijs kunnen voorkomen? Want het voorkomen van criminaliteit zorgt voor een betere veiligheid op de Hoog risico faciliteiten van de Deelnemers.

Om willekeur te voorkomen toetst Stichting Gatekeeper of een Maatregel conform dit protocol wordt toegepast. Stichting Gatekeeper beoordeelt verder alleen die specifieke Kaartgebruikers over wie zij zelf een melding van een Deelnemer of van politie of het Openbaar Ministerie ontvangt.

Noodzaak en evenredigheid

De Geautoriseerde functionaris van een Deelnemer en de directie van Stichting Gatekeeper dienen te beoordelen of de voorgenomen Maatregel noodzakelijk en evenredig is voor het verwezenlijken van het doel, namelijk voorkomen van fraude en criminaliteit bij de Deelnemers, wat zal zorgen voor een veilige werkplek op de Hoog risico faciliteiten van de Deelnemers. Ze dienen hierbij in ieder geval in te gaan op:

a. **Noodzakelijkheid**: zijn de verwerking van de Persoonsgegevens en onderlinge uitwisseling van Persoonsgegevens noodzakelijke handelingen om Kaartgebruikers die gedrag vertonen dat kwalificeert als Gedragingen, de toegang tot Hoog risico faciliteiten te beperken?

b. **Proportionaliteit**: staat de inbreuk op de persoonlijke levenssfeer, de bescherming van de Persoonsgegevens en de mogelijkheid zich van een inkomen te voorzien van de betrokken Kaartgebruiker in evenredige verhouding tot de voorgenomen Maatregel?

c. **Subsidiariteit**: kan het doel, zorgen voor een veilige werkplek op de Hoog risico faciliteiten van de Deelnemers, in redelijkheid niet op een andere, voor de betrokken Kaartgebruiker minder nadelige wijze, worden verwezenlijkt?

Noodzakelijkheid

De Maatregel moet noodzakelijk zijn om de veiligheid van medewerkers te waarborgen, criminaliteit en fraude tegen te gaan (zoals wordt verwacht door de overheid) en de onderneming voort te kunnen zetten. Onderzocht moet worden of meerdere Deelnemers worden geraakt. Ook is van belang of, zonder tijdige signalering, een aaneenschakeling van samenhangende of gelijksoortige fraude en criminaliteit kan plaatsvinden. Als criminelen vrij spel hebben of hun activiteiten zouden kunnen verplaatsen naar een andere Deelnemer, dan is het delen van informatie en waarschuwen binnen het Afsprakenstelsel noodzakelijk.

Proportionaliteit

De Maatregel moet proportioneel zijn met als uitgangspunt dat de veiligheid is gewaarborgd van de personen die zich bevinden binnen een Hoog risico faciliteit van een van de Deelnemers. Dit betreft de vraag naar effectiviteit en evenredigheid.

Effectiviteit

Indien de Deelnemer in redelijkheid verwacht dat met de Maatregel het gestelde doel wordt bereikt, dan is de Maatregel effectief.

Evenredigheid

De Maatregel volgt altijd op meldingen van een Deelnemer (in uitzonderingsgevallen van politie of het Openbaar Ministerie) waaruit blijkt dat gedrag van de Kaartgebruiker in kwestie kwalificeert als Gedragingen. De beperkte toegang zal meerdere Hoog risico faciliteiten van meerdere Deelnemers omvatten. Beoordeeld moet worden of de Kaartgebruiker nog steeds in zijn inkomen kan voorzien, bijvoorbeeld omdat hij wel toegang heeft tot de faciliteiten die niet onder een hoog risico vallen. Meegewogen moet worden dat Kaartgebruikers de mogelijkheid hebben om een Maatregel aan te vechten door een klacht in te dienen, bezwaar te maken of beroep in te dienen bij Stichting Gatekeeper. Het is aan de werkgever van de Kaartgebruiker om af te wegen of hij zulk gedrag toelaatbaar vindt in het kader van de werkzaamheden van de Kaartgebruiker. De reikwijdte van het delen van Strafrechtelijke Persoonsgegevens binnen het Afsprakenstelsel is beperkt tot de Deelnemers en alleen Geautoriseerde personen hebben toegang tot dossiers[23]. Om willekeur te voorkomen toetst Stichting Gatekeeper of een Maatregel conform dit protocol wordt toegepast.

Subsidiariteit

Subsidiariteit betreft de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze kan worden bereikt. Bijvoorbeeld door de toegang niet te beperken tot alle Hoog risico faciliteiten, maar tot een of enkele. Echter, personen die misbruik maken van het logistieke stelsel beperken hun activiteiten zelden tot een enkele Deelnemer. Bij fraude en criminaliteit zijn of worden vaak meerdere Deelnemers geraakt. Indien zonder tijdige signalering een aaneenschakeling van samenhangende of gelijksoortige fraude en criminaliteit kan plaatsvinden, is het delen van informatie en waarschuwen binnen het Afsprakenstelsel essentieel.

Overige overwegingen rond rechtvaardige inbreuk op de persoonlijke levenssfeer van de betrokken Kaartgebruikers

1. Het verwerken van Strafrechtelijke Persoonsgegevens is gevoelig en kan leiden tot stigmatisering en uitsluiting van individuele Kaartgebruikers. Daarom is terughoudendheid geboden.
2. Deelnemers mogen strafrechtelijke Persoonsgegevens slechts met elkaar delen op basis van dit protocol en de daarmee samenhangende verstrekte vergunning van de Autoriteit Persoonsgegevens.
3. De inbreuk op de persoonlijke levenssfeer van de Kaartgebruiker dient beperkt te blijven, onder meer doordat binnen het Afsprakenstelsel alleen een beperkt aantal personen toegangsrechten hebben tot de beveiligde Persoonsgegevens.
4. De bescherming van de Persoonsgegevens van de betrokken Kaartgebruikers wordt gewaarborgd omdat de Persoonsgegevens binnen het Afsprakenstelsel in een veilige

[23] Kamerstukken II 2017-18, 34 851, nr. 7, Nota naar aanleiding van het verslag, p. 55.

omgeving worden verwerkt met maximale aandacht voor vertrouwelijkheid en informatiebeveiliging.

5. Het Afsprakenstelsel waarborgt de rechten van de betrokken Kaartgebruiker, onder meer doordat hij de gebruikelijke AVG rechten (zoals inzage) kan uitoefenen. Dit is beschreven in de publieke Privacy Statements van de Deelnemers en op de website van Stichting Gatekeeper.
6. De website van Stichting Gatekeeper vermeldt de op het Afsprakenstelsel toepasselijke reglementen en procedures voor klachten, bezwaar en beroep.

Klachtenprocedure

Nadat een Kaartgebruiker een klacht heeft ingediend, treedt de klachtenprocedure in werking. Deze bestaat uit de volgende stappen.

1. Nadat een Kaartgebruiker een klacht heeft ingediend, beoordeelt de directie van Gatekeeper eerst of de klacht behandeld kan worden. Het kan zijn dat de directie daar meer informatie voor nodig heeft. Die informatie vraagt de directie op bij de Kaartgebruiker.
2. De directie van Gatekeeper spant zich in om de Kaartgebruiker te berichten of de klacht in behandeling wordt genomen binnen één week nadat de klacht is ingediend.
3. Als de klacht betrekking heeft op het beperken van toegang tot de faciliteiten van een enkele Deelnemer, dus niet op beperking van toegang tot meerdere Deelnemers, dan kan de directie van Gatekeeper de klacht niet behandelen. De Kaartgebruiker wordt gevraagd zijn klacht zelf voor te leggen aan de betreffende Deelnemer.
4. Als de directie van Gatekeeper de klacht om andere redenen niet kan behandelen, dan legt zij aan de Kaartgebruiker de redenen uit.
5. Als Stichting Gatekeeper de klacht kan behandelen, laat zij de klacht onderzoeken door een commissie van experts. Indien nodig schakelt zij daarbij de hulp in van een of meer Geautoriseerde functionarissen. Daarna volgt een beslissing. De beslissing op de klacht zal zijn:
   a) de Maatregel in stand houden;
   b) de Maatregel verkorten in duur;
   c) de Maatregel opschorten;
   d) de Maatregel opheffen.
6. Stichting Gatekeeper informeert de Kaartgebruiker zo snel mogelijk over de beslissing.

Bezwaar

Indien een Kaartgebruiker het niet eens is met de beslissing op zijn klacht, heeft de Kaartgebruiker het recht om tegen de beslissing bezwaar in te dienen bij de Geschillencommissie van Stichting Gatekeeper. Dat kan via de website van Stichting Gatekeeper. De voorzitter van de Geschillencommissie zal leden van de behandelende commissie aanwijzen om de klacht te behandelen en te beoordelen. De Geschillencommissie zal het bezwaar behandelen conform het reglement van de Geschillencommissie. De Geschillencommissie beslist onafhankelijk van de directie van Stichting Gatekeeper op het bezwaar. Bij het benoemen van een lid van de behandelende commissie kijkt de voorzitter naar de aard en de inhoud van de klacht en welke deskundigheid nodig voor de behandeling ervan. Bij de behandeling van de klacht kijkt de Geschillencommissie ook naar het financiële en maatschappelijke belang van de klacht en of er al eerder uitspraken zijn gedaan in vergelijkbare klachten. Een lid van de Geschillencommissie neemt geen deel aan de behandeling van een klacht als hij daar direct

of indirect een belang bij heeft. Mocht een (in)direct belang van een lid tijdens de behandeling van de klacht blijken, dan trekt dit lid zich terug uit de Geschillencommissie voor de duur van deze behandeling.

Beroep

Indien de Kaartgebruiker het niet eens is met de beslissing op zijn bezwaar, heeft de Kaartgebruiker het recht om tegen de beslissing beroep in te dienen bij de Commissie van Beroep van Stichting Gatekeeper. Dat kan via de website van Stichting Gatekeeper. De Commissie van Beroep zal het beroep behandelen conform het reglement Commissie van Beroep. De commissie neemt, onafhankelijk van de directie van Stichting Gatekeeper een beslissing op het beroep.

Indien een geschil niet leidt tot een oplossing kan de Kaartgebruiker zich wenden tot (i) de Autoriteit Persoonsgegevens en/of (ii) de bevoegde rechter.

Reglement Geschillencommissie en reglement Commissie van Beroep

Het reglement van de Geschillencommissie en van de Commissie van Beroep zijn van toepassing. Deze zijn te vinden op www.stichtinggatekeeper.nl.

Regels voor toetreding, uittreding en uitsluiting van het Afsprakenstelsel Gatekeeper

1. **Toetreding**. Een Deelnemer heeft het recht om toe te treden tot het Afsprakenstelsel indien de Deelnemer voldoet aan de in dit protocol opgestelde vereisten. Voorafgaand aan de toetreding dient de Deelnemer bij de Autoriteit Persoonsgegevens een vergunning aan te vragen op basis van dit protocol. Voor toetreding dient de Deelnemer een toetredingsovereenkomst te tekenen met Stichting Gatekeeper, waarin de Deelnemer onder meer verklaart dit protocol te zullen naleven en zich aan de toetredingsovereenkomst te zullen houden.
2. **Vrijwillige uittreden**. Een Deelnemer heeft het recht uit het Afsprakenstelsel te treden. Een Deelnemer dient zijn wens tot uittreding schriftelijk bij Stichting Gatekeeper kenbaar te maken onder vermelding van de gewenste datum van uittreding. Vanaf die datum zal Stichting Gatekeeper de ex-Deelnemer technisch afsluiten.
3. **Uitsluiting**. Als een Deelnemer niet langer aan de criteria van het protocol voldoet, zal de directie van Stichting Gatekeeper deze Deelnemer uitsluiten van deelname aan het Afsprakenstelsel. De directie van Stichting Gatekeeper zal deze Deelnemer technisch afsluiten.
4. **Overzicht Deelnemers, toetreders en uittreders**. Stichting Gatekeeper houdt een actueel overzicht bij van Deelnemers, toetreders en uittreders en publiceert dit op de website www.stichtinggatekeeper.nl waar het voor iedereen toegankelijk is. Een melding aan de Autoriteit Persoonsgegevens van uittreders is niet nodig. Zie verder de toepasselijke regels voor toezicht, audit, evaluatie en wijzigingen, zoals hieronder beschreven.

Algemene regels Afsprakenstelsel Gatekeeper

1. Deelnemers zijn ten aanzien van elkaar en ten aanzien van Stichting Gatekeeper gehouden tot naleving van dit protocol.
2. Deelnemers verlenen elkaar en Stichting Gatekeeper desgevraagd bijstand in het geval van vorderingen of verzoeken in verband met de rechten van Kaartgebruikers rond Persoonsgegevens.
3. Een Deelnemer die gegevens laat verwerken in het Centraal Incidentenregister Gatekeeper is aansprakelijk voor schade die ontstaat doordat de gegevens door deze

Deelnemer niet conform dit protocol zijn verwerkt in het Centraal Incidentenregister Gatekeeper, tenzij deze tekortkoming in de nakoming de Deelnemer niet kan worden toegerekend.

4. De Deelnemer die gegevens verwerkt die de Deelnemer via het Centraal Incidentenregister Gatekeeper heeft verkregen, is aansprakelijk voor schade die ontstaat doordat hij onjuist of disproportioneel gebruik van deze gegevens heeft gemaakt, tenzij deze tekortkoming in de nakoming de Deelnemer niet kan worden toegerekend.
5. Deelnemers zullen de werkwijze zoals neergelegd in dit protocol concretiseren binnen hun bedrijf.
6. Wanneer er sprake is van een misdrijf zal de betreffende Deelnemer aangifte doen bij een opsporingsambtenaar.

Regels voor rechten van betrokken Kaartgebruikers

1. Een Kaartgebruiker heeft recht op mededeling van opname in het Incidentenregister.
2. Het protocol kan worden opgevraagd bij Stichting Gatekeeper en is terug te vinden op de website van Stichting Gatekeeper.
3. De Kaartgebruiker heeft recht op inzage van zijn Persoonsgegevens in het Incidentenregister. Geen inzage wordt verstrekt, indien sprake is van een uitzonderingssituatie als bedoeld in artikel 41 UAVG. Dit is onder meer het geval bij voorkoming, opsporing en vervolging van strafbare feiten of de bescherming van de Kaartgebruiker of de rechten en vrijheden van anderen.
4. Verzoek om inzage moet schriftelijk worden ingediend en gelegitimeerd.
5. Stichting Gatekeeper moet, conform artikel 12 lid 3 AVG, onverwijld, en in ieder geval binnen een maand, reageren op het inzageverzoek.
6. Correctie en aanvulling van onjuiste Persoonsgegevens is mogelijk.
7. De Kaartgebruiker heeft recht op beperking van de verwerking van zijn Persoonsgegevens.
8. De Kaartgebruiker kan bezwaar maken op basis van bijzondere persoonlijke omstandigheden.
9. De Verwerkingsverantwoordelijke beoordeelt het bezwaar en beëindigt de verwerking indien nodig.
10. Bij een geschil over de juistheid en rechtmatigheid van de verwerking van Persoonsgegevens in het decentrale Incidentenregister van de betreffende Deelnemer kan de Kaartgebruiker zich wenden tot deze Deelnemer.
11. Bij een geschil over de juistheid en rechtmatigheid van de verwerking van Persoonsgegevens in het Centraal Incidentenregister Gatekeeper door Stichting Gatekeeper onder de reikwijdte van dit protocol kan de Kaartgebruiker zich wenden tot Stichting Gatekeeper.
12. Indien deze stap niet leidt tot een oplossing van het geschil kan de Kaartgebruiker zich wenden tot (i) de Geschillencommissie van Stichting Gatekeeper (en daarna de Commissie van Beroep) (ii) de AP; of (iii) de bevoegde rechter.

Regels voor toezicht, audit, evaluatie, verlenging vergunning en wijzigingen

1. Stichting Gatekeeper heeft een Functionaris voor de Gegevensbescherming (FG) aangesteld.
2. De directie van Stichting Gatekeeper staat onder toezicht van een raad van toezicht die 1 tot 4 keer per jaar vergadert. Daarnaast wordt de directie van Stichting Gatekeeper geadviseerd en gecontroleerd door een raad van advies die 1 tot 4 keer

per jaar vergadert. De directie van Stichting Gatekeeper laat zich verder bijstaan door een auditcommissie die tot taak heeft het periodiek laten uitvoeren van controlewerkzaamheden (audits) over het gebruik van Persoonsgegevens in het kader van de verplichtingen die voortvloeien uit dit protocol, de AVG, de Uitvoeringswet AVG of andere toepasselijke wet- en regelgeving door de Deelnemers en Stichting Gatekeeper zelf. De auditcommissie bestaat uit drie onafhankelijke personen waarbij tenminste één persoon lid is van de raad van toezicht. De Deelnemers en Stichting Gatekeeper verbinden zich alle gevraagde informatie aan de auditcommissie te verstrekken die voor de goede uitvoering van haar taak noodzakelijk is. De auditcommissie brengt van haar werkzaamheden en bevindingen in ieder geval één keer per jaar - en indien nodig vaker - verslag uit aan de directie van Stichting Gatekeeper.

3. Stichting Gatekeeper en de Deelnemers zijn gebonden de naleving van dit protocol periodiek (in ieder geval elke 3 jaar na toelating van een Deelnemer tot het Afsprakenstelsel Gatekeeper) te (laten) beoordelen en hierover te rapporteren.
4. Indien wordt vermoed dat een Deelnemer zich niet houdt aan de bepalingen van dit protocol dient dit door Stichting Gatekeeper te worden onderzocht. Stichting Gatekeeper stelt hierover een rapport op waarvan vertrouwelijk verslag dient te worden gedaan aan de directie van het betreffende Deelnemer.
5. Wanneer de auditcommissie verbeterpunten constateert, zal Stichting Gatekeeper de betreffende Deelnemer adviseren de betreffende verbeterpunten op te lossen binnen een bepaalde termijn. Indien een Deelnemer bij voortduring niet aan de in het kader van de verplichtingen die voortvloeien uit dit protocol, de AVG, de Uitvoeringswet AVG of andere toepasselijke wet- en regelgeving voldoet, zal Stichting Gatekeeper de betreffende Deelnemer uitsluiten van het Afsprakenstelsel en het openbare overzicht van Deelnemers op de website www.stichtinggatekeeper.nl aanpassen. Pas na aangetoonde verbetering kan een ex-Deelnemer weer toetreden tot het Afsprakenstelsel.
6. Deelnemers zijn vaak verplicht beveiligings- en veiligheidsbeleid op te stellen. Dit wordt gecontroleerd door de bevoegde instanties[24]. Specifiek voor zeehavens zijn ISPS-bedrijven havenbedrijven die internationaal scheepverkeer afhandelen. Zij zijn verplicht een toegangsbeleid te voeren voor de veiligheid en beveiliging van schepen en havenfaciliteiten. Daarbij verwerken zij persoonsgegevens. Zie in dit verband ook de Gedragscode Toegangsbeleid ISPS bedrijven[25].
7. De Autoriteit Persoonsgegevens verleent de vergunning op basis van dit protocol voor vijf jaar. Na vier jaar zal een verlengingsaanvraag worden ingediend bij de AP. Daarbij zal een afschrift van een privacy auditrapport toegezonden worden waaruit blijkt dat de Deelnemers nog steeds conform de in dit protocol omschreven wijze persoonsgegevens verwerken.
8. Dit protocol kan alleen worden aangepast indien de aanpassingen of wijzigingen niet op bezwaren zijn gestuit bij de Autoriteit Persoonsgegevens. Voor de aanpassingen en wijzigingen dient opnieuw een vergunning bij de Autoriteit Persoonsgegevens te worden verkregen.

[24] Bij zeehavens is dit bijvoorbeeld de International Ship and Port Security (ISPS) Code, op basis van Europese Richtlijn 725/2004 over verbetering van de beveiliging van schepen en havenfaciliteiten. Het lokale Havenbedrijf is dan de controlerende instantie.

[25] https://www.autoriteitpersoonsgegevens.nl/documenten/besluit-gedragscode-toegangsbeleid-isps-bedrijven