



> Retouradres Postbus 20701 2500 ES Den Haag

Bestuursstaf
Directie Communicatie

Kalvermarkt 32
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Contactpersoon
mr. S.J.L. Crombach

Datum **20 DEC 2021**
Onderwerp Besluit op uw Wob-verzoek

Geachte [REDACTED]

Bij brief van 5 augustus 2021 heeft u een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (Wob). In uw verzoek vraagt u naar informatie over het gebruik en de werking van algoritmes bij de Koninklijke Marechaussee (hierna: KMar). Op 19 oktober 2021 hebben de Wob-functionaris en de KMar met u een gesprek gehad. U heeft uw verzoek nader gespecificeerd en u vraagt nu om een lijst van indicatoren die worden omgezet in algoritmes. Daarnaast vraagt u om Data Protection Impact Assessments (DPIA's) van systemen waarin gebruik wordt gemaakt van dergelijke algoritmes.

Inventarisatie documenten

In antwoord op uw verzoek heb ik een inventarislijst opgesteld van de door u gevraagde documenten. De inventarislijst is als bijlage bij dit besluit gevoegd. In dit besluit verwijs ik naar de corresponderende nummers op de inventarislijst.

Algoritmes bij de KMar

De KMar heeft verschillende systemen met algoritmes op basis van bijvoorbeeld (risico)profielen of een set van indicatoren. Een profiel of een set van indicatoren worden in beginsel opgesteld aan de hand van kwalitatief onderzoek, bijvoorbeeld op grond van een 'intelligence report' of informatie uit bepaalde systemen. De KMar gebruikt geen zelflerende algoritmes waarop automatische besluitvorming volgt. Dat betekent dat het altijd de individuele KMar-medewerker is die besluit om eventueel, na een treffer in een van de systemen, een persoon of voertuig te controleren.

Besluit

Ik maak het formulier voor het opstellen van een profiel (document 5) en een procesbeschrijving van de wijze waarop profielen binnen de KMar worden gebruikt (document 6) volledig openbaar. Het Kwaliteitskader Big Data (document 3), het kader voor het opstellen van profielen, is reeds openbaar, maar is ook als bijlage bij dit besluit gevoegd. Daarnaast maak ik een 'intelligence report' (document 2) en een profiel van kindscherm (document 7) deels openbaar. Verder maak ik een DPIA van het slimme camerasysteem Amigoboras deels openbaar. Deze DPIA is overigens nog niet formeel vastgesteld en is daarom strikt genomen nog een concept. De DPIA van het systeem Advance Passenger Information (hierna: API) maak ik niet openbaar, omdat dit een concept is dat zich nog in de ontwikkelingsfase bevindt.

U heeft ook gevraagd om een lijst van indicatoren die de KMar gebruikt bij het programmeren van algoritmes in de systemen. Een dergelijke lijst bestaat niet en kan ik daarom niet openbaar maken. Afhankelijk van de omstandigheden worden verschillende indicatoren gebruikt.

Onze referentie
BS2021026296

Bijlagen
7

*Bij beantwoording datum,
onze referentie en onderwerp
vermelden.*



Ik licht hierna per uitzonderingsgrond als bedoeld in de artikelen 10 en 11 van de Wob toe waarom ik bepaalde documenten niet of deels openbaar maak.

Bestuursstaf
Directie Communicatie

Opsporing en vervolging van strafbare feiten & inspectie, controle en toezicht (artikel 10, tweede lid, aanhef en onder c en d)

Op grond van artikel 10, tweede lid, aanhef en onder c, van de Wob blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van opsporing en vervolging van strafbare feiten. Hierbij gaat het niet alleen om concrete gevallen, maar ook om dat belang in het algemeen. Bij de uitzonderingsgrond als bedoeld in voormeld artikellid, aanhef en onder d, gaat het om het belang van een doeltreffende inspectie, controle en toezicht, gericht op het vaststellen van niet-strafbare feiten.

Datum
20 DEC 2021
Onze referentie
BS2021026296

Ik maak op grond van artikel 10, tweede lid, aanhef en onder c en/of d, van de Wob documenten 1, 2 en 7 deels openbaar. Document 1 bevat informatie over hoe het slimme camerasysteem Amigoboras wordt gebruikt, zoals op welke wijze de passerende voertuigen worden geassocieerd en waar de camera's zijn opgesteld. Document 2 is een 'intelligence report', waarin een bepaalde trend wordt gesignaleerd en geanalyseerd. Document 7 is een profiel over kindsmokkel, waarin een bepaalde vorm daarvan wordt geanalyseerd en waarbij een aantal indicatoren worden vermeld. De gelakte informatie in deze documenten biedt niet alleen inzicht in de informatiepositie van de KMar, maar ook in de strategie en tactieken die de KMar gebruikt bij het bewaken van de grens en de daarmee samenhangende opsporing en vervolging van strafbare feiten. Openbaarmaking van deze informatie kan de effectiviteit van de KMar bij de uitoefening van deze taken in gevaar brengen. Als personen of groeperingen op de hoogte raken van de wijze waarop de KMar controle en toezicht uitoefent aan de grens of de opsporing en vervolging van strafbare feiten vormgeeft, kunnen zij daarop anticiperen. Dat kan ertoe leiden dat het zicht van de KMar op de grens en grenscriminaliteit, zoals mensensmokkel- en handel, verslechtert en de opsporing en vervolging van strafbare feiten belemmeren. Gelet hierop wegen de belangen van opsporing en vervolging van strafbare feiten en van inspectie, controle en toezicht zwaarder dan het belang van openbaarheid.

Eerbiediging van de persoonlijke levenssfeer (artikel 10, tweede lid, aanhef en onder e)

In document 1 staan persoonsgegevens van medewerkers van Defensie, zoals namen, telefoonnummers en e-mailadressen. Deze persoonsgegevens maak ik op grond van artikel 10, tweede lid, aanhef en onder e, van de Wob niet openbaar. Deze medewerkers treden niet wegens hun functie in de openbaarheid, zodat het belang van de eerbiediging van hun persoonlijke levenssfeer zwaarder weegt dan het belang van openbaarheid.

Het voorkomen van onevenredige bevoordeling of benadeling (artikel 10, tweede lid, aanhef en onder g)

In document 1 maak ik een aantal bedrijfsnamen op grond van artikel 10, tweede lid, aanhef en onder g, van de Wob niet openbaar. Openbaarmaking van deze bedrijfsnamen kan, gelet op de gevoelige aard en de inhoud van het document, leiden tot onevenredige benadeling van de betrokken bedrijven leiden.



Intern beraad met de daarin opgenomen persoonlijke beleidsopvattingen (artikel 11)

Artikel 11, eerste lid, van de Wob bepaalt dat uit documenten, opgesteld ten behoeve van intern beraad, geen informatie wordt verstrekt over daarin opgenomen persoonlijke beleidsopvattingen. Onder 'persoonlijke beleidsopvattingen' wordt verstaan: ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van het intern beraad. Dergelijke opvattingen worden niet openbaar gemaakt omdat een zekere mate van veiligheid en vertrouwelijkheid noodzakelijk is om te kunnen komen tot een effectieve besluitvorming. De persoonlijke beleidsopvattingen die onleesbaar zijn gemaakt bevatten geen beleidsalternatieven, prognoses en feiten.

Bestuursstaf
Directie Communicatie

Datum
20 DEC 2021
Onze referentie
BS2021026296

Concepten worden beschouwd als persoonlijke beleidsopvattingen, opgesteld voor het intern beraad. Document 4 is een concept-DPIA van het systeem API, dat zich nog in een vroege fase van ontwikkeling bevindt. Openbaarmaking van dit concept komt niet ten goede aan een goede bestuursvoering. Daarom maak ik document 4 op grond van artikel 11, eerste lid, van de Wob niet openbaar.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

De Minister van Defensie
voor deze
De Secretaris-Generaal.

Mr. G.E.A. van Craaijkamp

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit bezwaar indienen bij de Minister van Defensie. Het bezwaarschrift dient te worden gericht aan Dienstencentrum Juridische Dienstverlening, Commissie advisering bezwaarschriften Defensie, Postbus 90004, 3509 AA Utrecht. Het bezwaarschrift moet zijn ondertekend, een dagtekening bevatten en van de naam en het adres van de indiener zijn voorzien. Uit het bezwaarschrift moet duidelijk blijken tegen welk besluit en op welke gronden bezwaar wordt gemaakt.



Koninklijke Marechaussee

Gegevensbeschermings- effectbeoordeling (PIA)

Amigoboras

Ministerie van Defensie / Koninklijke Marechaussee

Staf CKMar / Directie Personeel & Bedrijfsvoering

Den Haag, oktober 2018



Ministerie van Defensie / Koninklijke Marechaussee – Staf CKMar / Directie DPB

Departementaal vertrouwelijk

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Minister van Defensie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Art. 10 (2) (e)

Advies CIO: Selecteer/typ datum

Naam: Typ naam/functie

Gegevensbeschermings- effectbeoordeling (PIA) Amigoboras

**Ministerie van Defensie / Koninklijke Marechaussee
Staf CKMar / Directie DPB**

Contact:

Ministerie van Defensie
Staf Koninklijke Marechaussee, PKC, Den Haag

AVG - coördinator

Art. 10 (2) (e)

Versie: 0.4 oktober 2018



PIA Amigoboras

Colofon

Versiebeheer

Versie	Datum	Status	Korte beschrijving wijziging
0.1	05-07-2018	Concept	Eerste concept
0.2	17-08-2018	Concept	Tweede concept, review resultaten verwerkt
0.3	14-09-2018	Concept	Derde concept, review resultaten vanuit JZ verwerkt
0.4	18-10-2019	Concept	Vierde concept, technische aanpassingen

Brondocumentatie

Titel	Versie	Datum	Auteur
Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)	1.0	september 2017	Ministerie van BZK, directie Constitutionele Zaken en Wetgeving
VIR E&E risicoanalyse Amigoboras	2.0	18 november 2010	Ministerie van Defensie Beveiligingsautoriteit
KOWA – Kmar Operationele Werkvloer Activiteiten	nvt	18 juni 2018	Koninklijke Marechaussee
Factsheet gebruik AmigoBoras	1.0	27 januari 2012	Koninklijke Marechaussee
CONOPS MTV	1.0	15 mei 2018	Koninklijke Marechaussee

Betrokken medewerkers

Bij het uitwerken van deze PIA zijn de volgende medewerkers betrokken:

Naam	Afdeling	Functie	Rol
Art. 10 (2) (e)	KMAR/STAF/DOPS/CL GRENSM	Beleidsadviseur	Beleidsadviseur
	KMAR/SPL/STAF/TCB	Coördinator EW&P	Materiedeskundige
	KMar/STAF/DOPS/Bur R&B	Wbp-coördinator	Jurist
	KMAR/SPL/STAF/TCB	Medewerker TCB	Materiedeskundige
	KMAR/STAF/KAB/CL JURZKN	Privacyfunctionaris	Jurist
	DMO/JIVC/VAM/INFO&ARCH/INFOMGMT	Informatiemanager	Systeemdeskundige
	KMAR/WEST/ST/SIE IV&C	Informatiemanager	Materiedeskundige
	DLBE/ST/SIE OPS/BRP/RMTLSOPROJ	Projectofficier (steller)	Projectmedewerker AVG/PIA
	DMO/OPS/AenA/DM1/UNIT3	Sr Projectmanager	Systeemdeskundige
	KMAR/STAF/DOPS	Directie Operations	Proces modeleigenaar
	KMAR/LTC/COGP/BASISGRH	Medewerker Intell	Materiedeskundige
	KMAR/STAF/DPB/CL ONDREAL/STC	Business analist	Business analist
	DMO/OPS/AenA/DM1/UNIT1	Projectmanager	OutputVerantw

Inhoudsopgave

Inleiding	8
A. Beschrijving kenmerken gegevensverwerkingen	9
1. Voorstel	9
2. Persoonsgegevens	12
3. Gegevensverwerkingen	13
4. Verwerkingsdoeleinden	15
5. Betrokken partijen	15
6. Belangen bij de gegevensverwerking	16
7. Verwerkingslocaties	16
8. Techniek en methode van gegevensverwerking	17
9. Juridisch en beleidsmatig kader	17
10. Bewaartermijnen	18
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	19
11. Rechtsgrond	19
12. Bijzondere persoonsgegevens	20
13. Doelbinding	20
14. Noodzaak en evenredigheid	20
15. Rechten van de betrokkene	21
C. Beschrijving en beoordeling risico's voor de betrokkenen	22
16. Risico's	22
D. Beschrijving voorgenomen maatregelen	23
17. Maatregelen	23

Externe bijlage: Samenwerkingsovereenkomst Amigoboras voor strafrechtelijke rechtshandhaving met betrekking tot grensoverschrijdende criminaliteit.

Inleiding

Op grond van artikel 4 lid 1 onder f van de Politiewet 2012 (Pw2012) en artikel 47 van de Vreemdelingenwet 2000 (Vw2000) is de Koninklijke Marechaussee (KMar) belast met het toezicht op de naleving van de wettelijke voorschriften met betrekking tot vreemdelingen. In dat kader voert de KMar in het grensgebied met België en Duitsland operationeel vreemdelingentoezicht uit, het zogenaamde Mobiel Toezicht Veiligheid (MTV). Het MTV wordt uitgevoerd op grond van artikel 50 Vw2000 en artikel 4.17a van het Vreemdelingenbesluit 2000 (Vb2000). Ter ondersteuning van het MTV maakt de KMar gebruik van het slimme camera-systeem Amigoboras, wat staat voor 'automatisch mobiel informatie gestuurd optreden – better operational result and advance security'. Het systeem omvat **Art. 10 (2) (c), Art. 10 (2) (d)** cameraopstellingen aan de wegen met België en Duitsland.

Amigoboras is primair bedoeld voor het uitvoeren van de MTV-taak. Daarnaast wordt het systeem door de KMar gebruikt voor de zelfstandige bestrijding van mensensmokkel en van fraude met reizen en identiteitsdocumenten (art. 4 lid 1 onder g Pw2012) en de bestrijding van grensoverschrijdende criminaliteit. In een samenwerkingsovereenkomst (externe bijlage) tussen de KMar en de politie is neergelegd dat Amigoboras kan worden ingezet voor de strafrechtelijke handhaving en in het bijzonder voor de aanpak van grensoverschrijdende criminaliteit. Deze inzet vindt haar juridische grondslag in art. 4 lid 1 onder d Pw2012, waarin de samenwerking en bijstand van de KMar aan de politie is geregeld.

Het uiteindelijke doel van Amigoboras is om de KMar-taken effectiever en efficiënter uit te kunnen voeren. Het systeem ondersteunt de KMar in het informatiegestuurd optreden.

Bij het gebruik van Amigoboras worden persoonsgegevens verwerkt. Daarbij is sprake van stelselmatige grootschalige monitoring en grootschalige gegevensverwerkingen. Vanuit die achtergrond is deze PIA tot stand gekomen. Informatie over de bescherming van persoonsgegevens is te vinden op het intranet van Defensie of op de internetpagina van de Autoriteit Persoonsgegevens.

Onderhavige PIA is als volgt tot stand gekomen:

1. Bestuderen van relevante en beschikbare (project)documentatie;
2. Bestuderen van de relevante informatie zoals opgenomen in het KOWA;
3. Het bevragen van deskundigen op het gebied van de werkprocessen en de operationele werking van Amigoboras;
4. Het bevragen van systeemdeskundigen, waaronder de outputverantwoordelijke van het systeem;
5. Het opstellen van een concept PIA, conform het standaardmodel van de Rijksoverheid;
6. Afstemming binnen het KMar implementatie project AVG-Wpg;
7. Het laten reviewen van de concept PIA door betrokkenen en het cluster juridische zaken van de KMar;
8. Het verwerken van de review-resultaten tot een definitieve PIA.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Object van de PIA: Amigoboras

Deze PIA ziet op het werkproces dat door Amigoboras wordt ondersteunt. Het slimme camera-systeem wordt ingezet voor de technische ondersteuning van:

- het MTV (art. 4 lid 1 onder f Pw2012);
- de bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten (art. 4 lid 1 onder g Pw2012);
- de verlening van bijstand alsmede de samenwerking met de politie (art. 4 lid 1 onder d Pw2012).

De taken worden hierdoor meer informatiegestuurd en daarmee efficiënter en effectiever uitgevoerd.

Achtergrond

Het Akkoord van Schengen uit 1985 heeft geleid tot de afschaffing van grenscontroles tussen de deelnemende landen. Met het oogmerk illegale immigratie en grensoverschrijdende criminaliteit tegen te gaan is in Nederland sinds 1994 de Koninklijke Marechaussee in het grensgebied belast met het MTV. Het MTV richt zich op reizigers die vanuit een ander Schengenland Nederland in reizen. Hoewel grenscontroles tussen de Schengenlanden zijn afgeschaft, moet eenieder wel zijn of haar identiteit, nationaliteit en verblijfsrechtelijke status kunnen aantonen. Heden ten dage vormt het MTV een onderdeel van het beleid van de Europese Unie, zoals vervat in het Integrated Border Management. Het MTV maakt deel uit van het zogenaamde Four Tier Acces Control Model, een barrièremodel gericht op het voorkomen en bestrijden van illegaal migratie.

Juridisch kader: taakstelling en bevoegdheid

Bij het overschrijden van de binnengrenzen van de lidstaten van de Europese Unie is de Schengengrenscore van toepassing. In artikel 22 is vastgelegd dat de binnengrenzen op iedere plaats kunnen worden overschreden zonder dat personen, ongeacht hun nationaliteit, worden gecontroleerd. In artikel 23 van de Schengengrenscore is bepaald dat de afschaffing van het grenstoezicht aan de binnengrenzen geen afbreuk doet aan de uitoefening van de politiebevoegdheid door de bevoegde instanties van de lidstaten overeenkomstig de nationale wetgeving, voor zover de uitoefening van die bevoegdheid niet hetzelfde effect heeft als grenscontroles. Dit geldt uitdrukkelijk ook in de grensgebieden.

Op grond van artikel 4 lid 1 onder f van de Politiewet 2012 en artikel 47 Vw2000 is de KMar belast met het toezicht op de naleving van de wettelijke voorschriften met betrekking tot vreemdelingen.¹ Voor deze taak berust het gezag over de KMar bij de minister van Justitie & Veiligheid. In dat kader voert de KMar in het grensgebied met België en Duitsland in het

¹ Uit artikel 1 van de Wet Politiegegevens (2018) moet worden begrepen dat de gegevensverwerking onder het AVG-regime valt.

grensgebied, dat strekt tot twintig kilometer vanaf de grens met de buurlanden, operationeel vreemdelingentoezicht uit, het zogenaamde MTV.

Amigoboras wordt primair toegepast voor het uitvoeren van de MTV-taak. Daarnaast wordt het systeem door de KMar gebruikt voor de zelfstandige bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten (art. 4 lid 1 onder g Pw2012) en de bestrijding van grensoverschrijdende criminaliteit. In een samenwerkingsovereenkomst (externe bijlage) tussen de KMar en de politie is neergelegd dat Amigoboras kan worden ingezet voor de strafrechtelijke handhaving en in het bijzonder voor de aanpak van grensoverschrijdende criminaliteit. Deze inzet vindt haar juridische grondslag in art. 4 lid 1 onder d Pw2012, waarin de samenwerking en bijstand van de KMar aan de politie is geregeld.

Deze MTV-controles zijn, conform de Schengengrenscore en de jurisprudentie van het Europese Hof op dit punt², wettelijk ingekaderd met betrekking tot de duur, tijdstip en frequentie.³

Het MTV wordt uitgevoerd op grond van artikel 50 Vw2000 en artikel 4.17a Vb2000. Het nationaal juridisch kader met betrekking tot MTV is volledig van toepassing op de ondersteuning die Amigoboras aan het toezicht biedt. In de vreemdelingenregelgeving zijn de controles qua intensiteit en frequentie ingekaderd. MTV kan worden uitgevoerd op Nederlands grondgebied, in de twintig kilometerzone op eenzelfde weg, ten hoogste negentig uur per maand en zes uur per dag. De bevoegdheden uit de vreemdelingenregelgeving geven geen specifieke basis voor de inzet van camera's of kentekenherkenning.

Functies van Amigoboras

Het systeem Amigoboras kent drie functies waarvan de werking hieronder wordt uitgewerkt. De beschrijving is bedoeld om de werking van Amigoboras duidelijk te maken.

Functie 1: Inwinnen en analyseren ten behoeve van profielen

Met de inwinfunctie worden aan de hand van inzetplannen gegevens verzameld over het grensverkeer. Passerende voertuigen worden door slimme sensoren geclassificeerd op

Art. 10 (2) (c), Art. 10 (2) (d)

. Bij Nederlandse kentekens worden de passagegegevens verrijkt door de database van de Rijksdienst voor het Wegverkeer (RDW) te raadplegen.⁴ De ingewonnen passagegegevens worden door Amigoboras gepseudonimiseerd⁵ en vervolgens, in een niet tot Amigoboras behorend datawarehouse⁶, verwerkt. Pseudonimiseren van passagegegevens houdt in dat het oorspronkelijke, tot de persoon te herleiden, kenteken met behulp van een versleutelingsmechanisme (hashing) wordt omgezet in een unieke waarde. Het oorspronkelijke kenteken wordt niet vastgelegd in het datawarehouse en is feitelijk niet meer te herleiden naar een natuurlijke persoon. Omdat de gegevens slechts gepseudonimiseerd worden en niet geanonimiseerd, betreft het hier nog steeds persoonsgegevens. De versleuteling is in het systeem geprogrammeerd en kan door de KMar niet worden aangepast, verwijderd of vernieuwd.

De passagegegevens worden gebruikt om door analyse risicoprofielen⁷ op te stellen, te verbeteren, en tevens trends en ontwikkelingen in de vervoersbewegingen te onderkennen. Dit laatste helpt de KMar in de planning en aansturing van later te houden MTV-controles. De risicoprofielen worden ingezet ter ondersteuning van het MTV. De risicoprofielen bevatten geen persoonsgegevens, maar zijn gericht op voertuigen en verkeersstromen. De inwinfunctie heeft geen directe rechtsgevolgen voor degenen van wie de passagegegevens worden verwerkt.

Functie 2: Observeren en selecteren voor het stilhouden van voertuigen

² Arrest Melki en Abdeli, C-188/10, C-189/10.

³ Art 50 Vreemdelingenwet 2000 juncto art 4.17a Vreemdelingenbesluit 2000.

⁴ Het gaat om een off-line database (kopie) van de RDW.

⁵ Conform art. 4 lid 5 AVG.

⁶ Basis Voorziening Informatie (BVI), het datawarehouse van de KMar.

⁷ In het Amigoboras systeem worden dit 'doelgroepdefinities' genoemd.

Amigoboras beschikt over een selectiefunctie. De selectiefunctie ondersteunt de KMar in het bepalen wie (welk voertuig) in aanmerking komt voor een controle. Het selecteren wordt gedaan door vooraf opgestelde profielen⁸ te vergelijken met het passerend verkeer. Wanneer een voertuig voldoet aan een profiel (een hit), zal het systeem een notificatie sturen naar de KMar-ambtenaren, die het voertuig vervolgens kunnen stoppen en de inzittenden controleren. Naast doelmatigheid en doeltreffendheid draagt het systeem ook bij aan de objectivering van de selectie. Het systeem is echter ondersteunend bedoeld. De KMar-medewerker besluit uiteindelijk welk voertuig voor controle wordt gestopt. De hits zijn bedoeld voor het direct uitvoeren van een MTV-controle en dienen daarom voor de duur van de actie in Amigoboras beschikbaar te zijn. Hits blijven 24 uur in het systeem beschikbaar.

Functie 3: Gericht kentekens zoeken in het grensgebied

Amigoboras kan worden ingezet om in het grensverkeer gericht naar kentekens te zoeken. Deze functie wordt gebruikt in het kader van het MTV.⁹ De juridische grondslag wordt gevonden in artikel 4 lid 1 onder f van de Pw2012 en artikel 47 Vw2000.

Op grond van artikel 4 lid 1 onder g Pw2012 kan de KMar van deze functie gebruik maken voor het tegengaan van illegale migratie en het zelfstandig bestrijden van identiteitsfraude en mensensmokkel. Een hit kan leiden tot daadwerkelijke opvolging of administratieve doormelding naar bijvoorbeeld een rechteerteam.

De mogelijkheid om gericht kentekens te zoeken kan eveneens worden aangewend ter assistentie van de politie in het kader van de rechtshandhaving en in het bijzonder de aanpak van grensoverschrijdende criminaliteit. Op grond van artikel 3 Pw2012 is de politie belast met de daadwerkelijke handhaving van de rechtsorde. Conform de tekst van artikel 4 lid 1 onder d Pw2012 is de KMar belast met de verlening van bijstand alsmede de samenwerking met de politie, daaronder begrepen de assistentieverlening aan de politie bij de bestrijding van grensoverschrijdende criminaliteit. Vanuit die achtergrond is in 2016 tussen de politie en de KMar een samenwerkingsovereenkomst afgesloten op het gebied van de inzet van Amigoboras voor rechtshandhaving in het grensgebied.¹⁰ Er zijn afspraken gemaakt over de inzet van Amigoboras voor de strafrechtelijke handhaving en in het bijzonder voor de aanpak van grensoverschrijdende criminaliteit bij wijze van assistentie van de KMar aan de politie.

In situaties waarbij sprake is van een bijzonder ernstige of omvangrijke inbreuk op de rechtsorde of de openbare orde of indien er sprake is van vitale hulpverleningsbelangen kan een kenteken voor een beperkte periode in Amigoboras worden opgenomen. Hierbij moet worden gedacht aan bijvoorbeeld een gijzeling, plofkraak, terrorisme of een amber alert. Er zijn concrete criteria vastgesteld voor het opnemen van Quick Alerts in Amigoboras. Een Quick Alert kan in het systeem worden ingevoerd als de betrokkene:

1. als verdachte kan worden aangemerkt van het plegen van een strafbaar feit waarop voorlopige hechtenis (art. 67 Sv) is toegestaan en is weggereden in een motorvoertuig waarvan het kenteken of een deel van het kenteken bekend is.
2. is weggereden in een motorvoertuig en heeft aangegeven dat hij/zij zich of een ander van het leven wil beroven.
3. is gekoppeld aan een Amber Alert.

In deze gevallen kan Amigoboras worden ingezet voor daadwerkelijke opvolging of administratieve doormelding van de hit. Een Quick Alert kan zowel voortkomen vanuit een zelfstandige KMar-taak als bij wijze van bijstandverlening aan de politie.

De relevantie van de Quick Alert functie is echter significant afgenomen door de samenwerkingsafspraken tussen de KMar en politie over de inzet van Amigoboras voor strafrechtelijke handhaving (externe bijlage).

Systeem-configuratie en beheersverantwoordelijkheden

⁸ Deze profielen zijn gebouwd op basis van de ingewonnen gegevens als beschreven in functie 1.

⁹ Er wordt in het kader van het MTV bijvoorbeeld gericht gezocht naar bepaalde autobussen.

¹⁰ Zie ook: Kamerstuk II 2013/14, 28 684, nr. 411.

Amigoboras is een systeem dat voor de eindgebruiker is ontsloten op de standaard kantooromgeving MULAN. Het systeem bestaat uit twee hoofdonderdelen, namelijk het sensordomein en een centrale applicatie.

Het sensordomein bestaat uit [] cameraopstellingen op [] locaties. De [] sensoren zijn geplaatst aan [] wegens in het grensgebied met België en Duitsland en zijn []. Naast [] beschikt de KMar over []. De fysieke camera's zijn het eigendom van defensie. De software die ervoor zorgt dat passagegegevens worden verzameld, verrijkt en doorgestuurd naar de centrale applicatie is eigendom van []. Deze partij verwerkt de gegevens voor de KMar. Er is echter geen verwerkersovereenkomst met [] afgesloten. Wel is de gegevensverwerker ABDO-geaccrediteerd.

De kern van Amigoboras wordt gevormd door de centrale applicatie waar alle passagegegevens vanuit het sensordomein binnenkomen en worden verwerkt voor de verschillende functies. De applicatie, die ontwikkeld is door Cap Gemini, draait binnen de IT-infrastructuur van defensie en wordt ook door defensie beheerd. De [] weginfra wordt beheerd door [] en Cap Gemini hebben geen rol in de gegevensverwerking.

Systeemfuncties separaat instelbaar

Om invulling te geven aan het beginsel 'privacy by design' kunnen systeemfuncties separaat worden ingesteld. Dit houdt in dat het systeem op onderscheiden fysieke locaties op een verschillende manier kan worden ingezet.

Buiten scope: vastleggen en bewaren van kentekens op grond van art. 126 jj Sv.¹¹

Art. 126jj van het Wetboek van Strafvordering regelt het vastleggen en bewaren van kentekengegevens door de politie. Deze regeling is ook van toepassing op het sensordomein van Amigoboras. Alle ruwe data afkomstig van de sensoren van Amigoboras, wordt voor de duur van 4 weken opgeslagen in een centraal kentekenregister (Argus). Het register is in beheer bij de politie. Op deze gegevensverwerking is de Wet Politiegegevens van toepassing. Raadpleging van deze gegevens is slechts onder voorwaarden mogelijk door geautoriseerde opsporingsambtenaren. Deze gegevensverwerking valt buiten het bestek van deze PIA.

Amigoboras is technisch in staat kentekens onversleuteld in te winnen en vervolgens te verwerken in het datawarehouse van de KMar. Deze functie wordt louter op last van de Officier van Justitie gebruikt. Met de inwerkingtreding van art. 126jj Sv. is te verwachten dat deze functie niet langer gebruikt wordt.

2. Persoonsgegevens

I

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

¹¹ Verwachte inwerkingtreding: 1 januari 2019.

Betrokkene	Categorie Persoonsgegevens	Typen Persoonsgegevens
Kentekenhouders - grenspassant	Kenteken	Gewoon
Kentekenhouders - gezocht kenteken	Kenteken gevaarclassificatie	Gewoon/ Strafrechtelijk
Contactpersoon bij hit	Contactgegevens	Gewoon
Medewerker (defensie)	Medewerkergegevens	Gewoon

Kentekenhouders - grenspassant

Het centrale attribuut in het gebruik van Amigoboras is het kenteken van een voertuig. Het kenteken is een gegeven dat tot een natuurlijk persoon herleidbaar kan zijn, namelijk de eigenaar of houder van het kenteken. In samenhang met het door de sensor gelezen kenteken kan ook Art. 10 (2) (c), Art. 10 (2) (d)

worden verwerkt. In het geval van Nederlandse kentekens worden de passagegegevens verrijkt met door op basis van het kenteken de database van de RDW te raadplegen.

Kentekenhouders - gezocht kenteken

In het systeem kunnen kentekens worden ingevoerd teneinde in het grensgebied een kenteken te zoeken. In het geval van een Quick Alert kan daarbij een gevaarclassificatie worden opgenomen.

Contactpersoon gericht kenteken zoeken

Bij het invoeren van een kenteken of Quick Alert in Amigoboras kan een contactpersoon worden geregistreerd. Er wordt dan een naam, e-mailadres en/of telefoonnummer geregistreerd om bij een grenspassage contact op te kunnen nemen en passagegegevens door te geven. Veelal wordt echter verwezen naar de Officier van Dienst – Informatie (OVD-I).

Medewerker

De gebruikers van het systeem zijn primair KMar-medewerkers. Secundair hebben ook beheerders van defensie toegang tot het systeem. Op accountniveau wordt het handelen vastgelegd. Een account is tot de persoon (medewerker) herleidbaar.

Opgemerkt wordt dat beheerders van het Art. 10 (2) (g) toegang hebben tot de gegevens in het sensordomein. Vanuit defensie is hier geen zicht op.

3. Gegevensverwerkingen

I

Geef alle voorgenomen gegevensverwerkingen weer.

Ten aanzien van het verwerken van gegevens met behulp van Amigoboras moet verschil worden gemaakt naar de twee delen waaruit het systeem bestaat, namelijk het sensordomein (cameraopstelling) en de centrale applicatie.

Door het door **Art. 10 (2) (g)** beheerde sensordomein worden kentekens en aanvullende passagegegevens verzameld van voertuigen die Nederland binnenkomen. Indien het om een Nederlands kenteken gaat, wordt de database van de RDW bevraagd om de passagegegevens met enkele elementen te verrijken. De verzamelde gegevens worden vanuit het sensordomein beveiligd verstuurd naar de centrale applicatie. Binnen de door defensie beheerde centrale applicatie vindt verdere gegevensverwerking plaats. Daarbij moet verschil worden gemaakt naar de drie verschillende toepassingen van het systeem:

1. Het inwinnen van gepseudonimiseerde gegevens: Ieder kenteken wordt gepseudonimiseerd naar een unieke code en in combinatie met de passagegegevens vanuit Amigoboras opgeslagen in het datawarehouse van de KMar. Met behulp van de gepseudonimiseerde gegevens worden profielen ontwikkeld. Het algoritme voor pseudonimisering is geprogrammeerd in Amigoboras. Op de gegevensverwerking in het kader van de inwinfunctie, waaronder het ontwikkelen van profielen, is de AVG van toepassing.
2. Observeren en selecteren van voertuigen voor mogelijke controle: De passagegegevens worden vergeleken met vooraf opgestelde profielen. Wanneer een passerend voertuig voldoet aan een profiel (een hit), zal het systeem een notificatie sturen naar de KMar-medewerkers, die het voertuig vervolgens ter controle kunnen stoppen. De hitgegevens worden binnen de centrale applicatie maximaal 24 uur bewaard en doorgestuurd naar het datawarehouse van de KMar. De overige passagegegevens worden vrijwel direct automatisch vernietigd. Op de gegevensverwerking in het kader van de selectiefunctie is de AVG van toepassing.
3. Gericht zoeken naar kentekens: Passagegegevens vanuit het sensordomein worden binnen de centrale applicatie vergeleken met kentekenlijsten. Bij een hit vindt een notificatie plaats. Dat kan leiden tot directe opvolging of administratieve doorgeleiding. Als de gegevensverwerking plaatsvindt in het kader van het MTV is de AVG van toepassing. In het geval de zoekfunctie naar kentekens wordt ingezet voor de zelfstandige bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten of de assistentieverlening van de KMar aan de politie is artikel 8 of 9 van de Wpg van toepassing. De hitgegevens worden binnen de centrale applicatie maximaal 24 uur bewaard en doorgestuurd naar een niet tot Amigoboras behorend datawarehouse. De overige passagegegevens worden vrijwel direct automatisch vernietigd.

Verwerking kentekens

Kentekenlijsten die door de KMar worden gebruikt in het kader van het MTV (art. 4 lid 1 onder f Pw2012) en het de bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten (art. 4 lid 1 onder g Pw2012) worden in beginsel elke 2 weken ververs. Bepaalde lijsten worden om proces-technische redenen maandelijks ververs. De kentekenlijsten worden aangeleverd vanuit de Intell-organisatie (Analyse & Onderzoek) en in het systeem ingevoerd door het Targetting Center Borders (TCB). Voor deze lijsten wordt steeds toestemming gegeven door een Officier van Justitie.

Kentekens die worden gezocht voor rechercheonderzoeken (zelfstandige KMar-taak of bijstand aan de politie) worden voor maximaal 3 maanden in het systeem gezet. Gegevensverwerking in het kader van rechercheonderzoeken vindt plaats op grond van art. 9 Wpg. Wanneer het kenteken eerder uit het systeem moet worden gehaald, wordt dit door het rechercheteam aangegeven. Het TCB voert de mutaties in het systeem handmatig uit. Kentekens worden alleen in het systeem gezet als er toestemming is gegeven door een Officier van Justitie.

Aan Quick Alerts wordt bij de invoer een beperkte geldigheidsduur verbonden. Na het verstrijken ervan is de Quick Alert niet langer actief. Het vernietigen van Quick Alerts

gebeurt handmatig na het verstrijken van de geldigheidsduur. De verwerking vindt plaats op grond van artikel 8 of 9 Wpg.

Verzoekprocedure kentekenopname

Een verzoek om een kenteken op een kentekenlijst (zelfstandige KMar-taak of bijstand aan de politie) te plaatsen, gebeurt middels een digitaal formulier. Naast het gezochte kenteken bevat het formulier informatie over de verzoekende instantie, de reden van het verzoek, mutatienummer van het politiesysteem, de wijze van opvolging, contactgegevens van de betrokken Officier van Justitie en contactgegevens van degene die bij hits geïnformeerd moet worden. De verzoeken worden, eventueel met tussenkomst van de Infodesk¹², verwerkt door het TCB. In Amigoboras wordt aan persoonsgegevens verwerkt: het kenteken en de naam, telefoonnummer en e-mailadres van de contactpersoon bij een hit.

Iedere aanvraag voor een Quick Alert wordt met behulp van een digitaal formulier ingediend bij het OPSCENT. Naast het gezochte kenteken bevat het formulier informatie over de verzoekende instantie, de reden van het verzoek, de periode waarin gezocht moet worden, het mutatienummer van het politiesysteem, de wijze van opvolging, eventuele gevarenclassificatie van de persoon, de eventueel betrokken Officier van Justitie en contactgegevens van degene die bij een hit geïnformeerd moet worden. De aanvraag wordt door het OPSCENT beoordeeld en eventueel ingevoerd. De persoonsgegevens van degene die het besluit neemt wordt op het formulier vastgelegd. In Amigoboras wordt aan persoonsgegevens verwerkt: het kenteken, eventueel een gevarenclassificatie van de persoon en de naam, telefoonnummer en e-mailadres van de contactpersoon bij een hit.

Archivering verzoekformulieren

De aanvraagformulieren om kentekens op een lijst te plaatsen en verzoeken tot Quick Alerts worden door het TCB in een functionele mailbox gearhiveerd. Op de inhoud van de formulieren is de Wpg van toepassing en geldt een bewaartermijn van een jaar is. Op kentekenlijsten die worden gebruikt in het kader van het vreemdelingtoezicht is de AVG van toepassing. Binnen het TCB wordt een schoningsprocedure gehanteerd: maandelijks worden de formulieren die ouder zijn dan 1 jaar uit de mailbox verwijderd. In het mailarchief van defensie blijven de formulieren echter bestaan.

Gegevensverwerking ten aanzien van medewerkers

Alle handelingen die medewerkers op Amigoboras uitvoeren worden op accountniveau en systeemniveau gelogd om te kunnen achterhalen wat er is gebeurt, indien daar aanleiding toe is. Er is geen bewaartermijn ingesteld of schoningsprocedure ingeregeld.

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Het doel van de gegevensverwerking met Amigoboras is om de KMar-taken effectiever en efficiënter uit te kunnen voeren. Het systeem ondersteunt de KMar in het informatiegestuurd optreden. Zie voor de verwerkingsdoeleinden per functie paragraaf 1.

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke,

¹² De politie dient de verzoeken in bij de Infodesk.

verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

De gegevens worden verwerkt in het kader van de wettelijke taken van de KMar. Hiervoor is de Minister van Defensie verantwoordelijk.

Zoals eerder aangegeven bestaat Amigoboras uit een centrale applicatie en een sensordomein. Bij de gegevensverwerkingen binnen de centrale applicatie is uitsluitend defensie betrokken. Het beheer van het sensordomein is neergelegd bij **Art. 10 (2) (g)**. [REDACTED] zorgt ervoor dat kentekens worden herkend, verrijkt en doorgestuurd naar de centrale applicatie. Die partij is daarmee gegevensverwerker voor defensie. Het ontbreekt echter aan een verwerkersovereenkomst. Wel is [REDACTED] ABDO-geaccrediteerd.

De gebruikers van Amigoboras zijn operationele medewerkers van de KMar. De toegang tot applicaties is bij Defensie ingericht via een autorisatiematrix¹³, zodat de toegang tot het strikt noodzakelijke wordt ingeperkt. Louter KMar-medewerkers met een relevante functie komen voor autorisatie in aanmerking. Binnen Amigoboras worden verschillende rollen onderkend, namelijk: regisseur, controleur, plan invoerder, plan goedkeurder, analist, watchlist/profiel maker en Quick Alert invoerder. Een gebruiker kan geautoriseerd zijn voor één of meerdere rollen. Naast operationele gebruikers hebben applicatiebeheerders en functioneel beheerders van defensie toegang tot de gegevens in Amigoboras.

Amigoboras wordt gebruikt in het kader van bijstandsverlening van de KMar aan de politie. De samenwerkingsovereenkomst (externe bijlage) geeft hier nader invulling aan.

De KMar verwerkt binnen Amigoboras kentekens die door de politie aan de KMar worden aangereikt (beschreven in paragraaf 3). De verwerking vindt plaats op grond van 8 of 9 Wpg. Bij een positieve vergelijking tussen een herkend kenteken en een kenteken op de lijst wordt de complete set aan passagegegevens via de e-mail aan de contactpersoon bij de politie toegestuurd. Ten overvloede: politiemedewerkers hebben zelf geen toegang tot het systeem.

6. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Het belang van de verwerkingsverantwoordelijke is het doelmatig en doeltreffend uitvoeren van de wettelijk opgedragen taken. Het optreden van de KMar moet leiden tot een veiliger Nederland, door het bestrijden van illegale migratie en grensoverschrijdende criminaliteit.

Het belang van andere partijen bij de gegevensverwerking in Amigoboras, te weten politie en openbaar ministerie, is het doeltreffend kunnen uitvoeren van politietaken door de politie en de strafvordering van het openbaar ministerie.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

¹³ Rule based access control.

De verwerkingen in Amigoboras vinden uitsluitend in Nederland plaats. De centrale applicatie is opgenomen in de ICT-architectuur van defensie. De verwerkingen binnen het sensordomein, onder beheer van Art. 10 (2) (g), vinden plaats op de verschillende cameralocaties en een centrale verwerkingslocatie van .

8. Techniek en methode van gegevensverwerking

I

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Amigoboras is in twee delen te splitsen, namelijk het sensordomein en de centrale applicatie. De gegevens die bij de grenspassage door de sensoren boven de weg worden verzameld worden versleuteld en via het internet en naar de centrale applicatie verzonden. Afhankelijk van de toepassing van het systeem worden de gegevens verwerkt.

1. Bij de inwinfunctie worden de passagegegevens door de centrale applicatie gepseudonimiseerd en vervolgens, in een niet tot Amigoboras behorend datawarehouse, verwerkt.
2. Bij de selectiefunctie worden de passagegegevens door de centrale applicatie vergeleken met vooraf opgestelde profielen. Wanneer een voertuig voldoet aan een profiel, zal het systeem een notificatie sturen naar de KMar-medewerkers, die het voertuig (op basis van de hit) ter controle kunnen stoppen.
3. Bij het gericht zoeken naar kentekens in het grensgebied worden passagegegevens door de centrale applicatie vergeleken met kentekenlijsten.

Er is binnen de systeemgrenzen van Amigoboras geen sprake van (semi)geautomatiseerde besluitvorming of big-data verwerkingen waarbij persoonsgegevens worden verwerkt. De door Amigoboras geproduceerde gepseudonimiseerde gegevens worden, door de Intell-organisatie van de KMar, in een datawarehouse verwerkt om profielen te ontwikkelen. De profielen worden vervolgens gebruikt (selectiefunctie) om het MTV doelmatiger en doeltreffender uit te voeren. Deze gegevensverwerking leidt echter niet tot rechtsgevolgen voor het individu waarvan gegevens worden verwerkt. De profielen bevatten geen persoonsgegevens en zijn gericht op vervoersmiddelen en vervoersbewegingen.

9. Juridisch en beleidsmatig kader

I

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

De taken van de KMar zijn neergelegd in artikel 4 van de Politiewet 2012. De Schengengrenscore geeft regels voor de overschrijding van grenzen door personen. Het MTV, waar Amigoboras primair ondersteunend aan is, is geregeld en afgebakend in de nationale vreemdelingenregelgeving. Naast het privacyregime van de AVG is ook de WPG van toepassing, omdat Amigoboras functies heeft waarbij politiegegevens worden verwerkt. Voor een omschrijving welke taken onder het regime van de Wpg vallen en welke taken onder het regime van de AVG vallen, wordt verwezen naar paragraaf 3.

Tussen de politie en de KMar is een samenwerkingsovereenkomst gesloten over het gebruik van Amigoboras op het gebied van de strafrechtelijke handhaving, in het bijzonder grensoverschrijdende criminaliteit. Voor een nadere toelichting zie de samenwerkingsovereenkomst (externe bijlage).

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Er dient onderscheid te worden gemaakt naar het sensordomein en de centrale applicatie. De door het sensordomein verzamelde gegevens worden in beginsel direct doorgestuurd naar de centrale applicatie om verwerkt te worden. Binnen het sensordomein kunnen de gegevens echter maximaal 2 uur worden bewaard om eventuele verbindingsproblemen met de centrale applicatie op te vangen.

In het kader van bewaartermijnen wordt verschil gemaakt naar de verschillende functies van de centrale applicatie:

1. Bij de inwinfunctie worden de gegevens 24 uur bewaard, gepseudonimiseerd en vervolgens, in een niet tot Amigoboras behorend datawarehouse, verwerkt. Binnen Amigoboras worden de gegevens automatisch vernietigd. Er is geen bewaartermijn bepaald voor de gepseudonimiseerde gegevens¹⁴ in het datawarehouse.
2. Bij de selectiefunctie blijven de hits beschikbaar voor de duur van de MTV-actie. De bewaartermijn is ingeregeld op 24 uur. De gegevens worden doorgestuurd naar het datawarehouse van de KMar en binnen Amigoboras automatisch vernietigd.
3. Kentekens op lijsten om in het grensgebied naar te zoeken worden zowel verwerkt op grond van de AVG (MTV) als artikel 8 en 9 Wpg (politietaken). Kentekenlijsten worden in beginsel elke 2 weken ververs. Bepaalde lijsten worden om proces-technische redenen maandelijks ververs. Kentekens die worden gezocht voor rechercheonderzoeken worden voor maximaal 3 maanden in het systeem gezet. Wanneer het kenteken eerder uit het systeem moet worden gehaald, wordt dit door het researcheteam aangegeven. Het TCB voert de mutaties in het systeem handmatig uit. Kentekens worden door het TCB alleen in het systeem gezet als er toestemming is gegeven door een Officier van Justitie.

Aan Quick Alerts wordt bij de invoer een (beperkte) geldigheidsduur verbonden. Na het verstrijken ervan is de Quick Alert niet langer actief. Het vernietigen van Quick Alerts gebeurt handmatig na het verstrijken van de geldigheidsduur. Gelet op de wetsgeschiedenis zal het hanteren van een beperkte termijn als hier niet snel leiden tot het aannemen van een verzuim als bedoeld in artikel 359a Sv.

Wanneer in het grensgebied een kenteken wordt herkend, blijft de hit 24 uur in Amigoboras beschikbaar. Digitale aanvraagformulieren om een kenteken op een lijst op te nemen en een verzoek voor een Quick Alert, worden bewaard in een functionele mailbox, waarop conform de Wpg een bewaartermijn van 1 jaar van toepassing is. Verwijderen van formulieren uit de mailbox gebeurt handmatig conform een maandelijks schoningsprocedure. In het mailarchief blijven de formulieren echter voor een periode van 5 jaar bewaard om vervolgens automatisch vernietigd te worden.

Wanneer een kenteken op een kentekenlijst wordt opgenomen, wordt ook een contactpersoon geregistreerd. Bij het vernietigen van het kenteken worden ook de contactgegevens uit het systeem vernietigd.

Gegevens van medewerkers worden op accountniveau bewaard om te kunnen terugzien wat op een bepaald moment is gebeurd. Beheerders hebben toegang tot de logging. Er is geen bewaartermijn bepaald en geen schoningsprocedure ingeregeld.

¹⁴ Dit zijn persoonsgegevens.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Gegevensverwerking in het kader van de vreemdelingentaak

Op grond van art. 4 lid 1 onder f van de Pw2012 en art. 47 Vw2000 is de KMar belast met het toezicht op de naleving van de wettelijke voorschriften met betrekking tot vreemdelingen. De Schengengrenscore geeft in art. 22 en 23 regels over het overschrijden van de binnengrenzen van de lidstaten. Nationaal rechtelijk wordt het toezicht uitgevoerd op grond van art. 50 Vw2000 en art. 4.17a Vb2000. Op het verzamelen van kentekens bij grenspassage is art. 6 lid 1 onder e AVG van toepassing: De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Uit art. 1 WPG (2018) blijkt expliciet dat de KMar-taak als benoemd in art. 4 lid 1 onder f van de Pw2012 geen politietask is.

Zoeken naar kentekens in het grensverkeer

Amigoboras kan worden gebruikt om in het grensverkeer verzamelde kentekens te vergelijken met een lijst met kentekens die worden gezocht. Krachtens artikel 4 Pw2012 kan de KMar van deze functie gebruikmaken voor het tegengaan van illegale migratie en de zelfstandige bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten. Deze functie kan eveneens worden gebruikt ter assistentie van de politie bij de aanpak van grensoverschrijdende criminaliteit. Op grond van artikel 3 Pw2012 is de politie belast met de daadwerkelijke handhaving van de rechtsorde. Conform de tekst van artikel 4 lid 1 onder d Pw2012 is de KMar belast met de verlening van bijstand alsmede de samenwerking met de politie, daaronder begrepen de assistentieverlening aan de politie bij de bestrijding van grensoverschrijdende criminaliteit. Kentekens die in Amigoboras worden opgenomen om daar in de grensregio gericht naar te zoeken, worden verwerkt op basis van art. 8 (uitvoering van de dagelijkse politietask) of art. 9 (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) van de Wpg.

In situaties waarbij sprake is van een bijzonder ernstige of omvangrijke inbreuk op de rechtsorde of de openbare orde of indien er sprake is van vitale hulpverleningsbelangen kan een kenteken

voor een beperkte periode als een Quick Alert in Amigoboras worden opgenomen. Een Quick Alert kan zowel voortkomen vanuit een zelfstandige KMar-taak als bij wijze van assistentieverlening aan de politie. De rechtsgrondslag voor een inladen van een Quick Alert wijkt niet af van de rechtsgrondslag om een kenteken op een lijst te zetten om daar in het grensgebied naar te zoeken, zoals in de vorige alinea beschreven.

12. Bijzondere persoonsgegevens

I

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Binnen Amigoboras worden hits verwerkt. Een hit is een positieve vergelijking tussen een herkend kenteken en een kenteken op een lijst dat op grond van artikel 8 of 9 Wpg is verwerkt. Een hit zegt iets over de strafrechtelijke achtergrond van betrokkene en is daarmee een bijzonder/strafrechtelijk persoonsgegeven. Het verwerken van een positieve vergelijking is op grond van de Wpg toegestaan.

In het kader van een Quick Alert kan een gevarenclassificatie van een persoon worden opgenomen. Een gevarenclassificatie zegt iets over de **Art. 10 (2) (c), Art. 10 (2) (d)** achtergrond van een persoon. Het verwerken van deze gegevens in het kader van de politietaken is op grond van de Wpg toegestaan.

13. Doelbinding

I

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De kentekens worden in beginsel verzameld en verwerkt in het kader van het vreemdelingentoezicht (art. 4 lid 1 onder f Pw2012), waarop de AVG van toepassing is. De verzamelde kentekens worden binnen Amigoboras tevens verwerkt voor andere aan de KMar opgedragen taken namelijk:

- de bestrijding van mensensmokkel en van fraude met reis- en identiteitsdocumenten (art. 4 lid 1 onder g Pw2012).
- de verlening van bijstand alsmede de samenwerking met de politie (art. 4 lid 1 onder d Pw2012).

Vanuit deze politietaken is de KMar op grond van art. 8 Wpg bevoegd kentekengegevens te verwerken. Het feit dat de KMar belast en bevoegd is om de verschillende taken aan de binnengrens uit te voeren maakt dat de verdere verwerking van kentekens verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Artikel 6 lid 4 van de AVG biedt ruimte voor deze verdere verwerking.

14. Noodzaak en evenredigheid

I

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- Proportionaliteit:** staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Subsidiariteit:** kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

De gegevensverwerking met behulp van Amigoboras is noodzakelijk om de wettelijk opgedragen taken (het MTV, het zelfstandig bestrijden van mensensmokkel en van fraude met reis- en identiteitsdocumenten, en de assistentieverlening aan de politie) doelmatig en doeltreffend uit te kunnen voeren; er wordt een gerechtvaardigd doel nagestreefd. De inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen door kentekens te verwerken staat in verhouding tot het te bereiken doel. Het is redelijkerwijs niet mogelijk het doel op een voor de betrokkene minder ingrijpende manier te bereiken.

Bij de inwinfunctie (ten behoeve van de ontwikkeling van MTV-profielen) worden ingewonnen kentekens nagenoeg direct gepseudonimiseerd. Deze verwerking heeft geen directe rechtsgevolgen voor het individu waarvan de gegevens zijn verzameld.

Bij de selectiefunctie vindt verwerking van kentekens uitsluitend plaats om doeltreffend en doelmatig MTV-controles uit te kunnen voeren. Na de MTV-actie worden de hit-gegevens uit Amigoboras verwijderd. In het geval van voornoemde functies is de inbreuk op de rechten van betrokkene klein, omdat er een helder afgebakend verwerkingsdoel bestaat en de bewaartermijn tot het minimum wordt beperkt.

De functie waarbij in het grensverkeer gericht wordt gezocht naar kentekens maakt een beperkte inbreuk op de bescherming van de persoonlijke levenssfeer zoals neergelegd in art. 10 Grondwet, art. 8 EVRM en art. 8 EU-Handvest van de grondrechten. De inbreuk is in relatie tot de te dienen doelen proportioneel. Er worden gerechtvaardigd doelen nagestreefd, namelijk vreemdelingtoezicht en strafrechtelijke handhaving, in het bijzonder de aanpak van grensoverschrijdende criminaliteit. De kentekens worden door een zeer beperkt aantal medewerkers van de KMar verwerkt, waardoor de inbreuk beperkt blijft. De kentekens blijven binnen Amigoboras niet langer beschikbaar dan strikt noodzakelijk is.

15. Rechten van de betrokkene



Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Op het verzamelen en nader verwerken van kentekens met Amigoboras is in beginsel de AVG van toepassing. De aanwezigheid van de permanente camera's wordt kenbaar gemaakt door middel van borden bij de cameraportalen. Daarnaast is voor iedereen op de internetpagina informatie over het systeem in relatie tot privacy beschikbaar. Om een bepaald recht uit te oefenen kan de betrokkene zich wenden tot de AVG-coördinator.

Wanneer in het kader van de politietaak in het grensverkeer naar kentekens wordt gezocht is de WPG van toepassing. In de artikelen 25 tot en met 28 zijn de rechten van de betrokkene neergelegd, namelijk het recht op verstrekking van informatie, inzage, rectificatie en vernietiging van politiegegevens. Een verzoek van een betrokkene wordt afgehandeld conform de OI 'Rechten Betrokkene Wet Politiegegevens'. Formulieren zijn te vinden op het intranet: http://intranet.mindef.nl/kmar/bedrijfsvoering/projecten/Wpg/Wpg_formulieren.aspx

Om een bepaald recht uit te oefenen kan de betrokkene zich wenden tot de Privacyfunctionaris.

Iedere betrokkene heeft het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

1

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- b. de oorsprong van deze gevolgen;
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Binnen Amigoboras is sprake van stelselmatige grootschalige monitoring en grootschalige verwerking van persoonsgegevens.

De systeemarchitectuur van Amigoboras maakt dat er geen duidelijk verschil is tussen de gegevensverwerking op grond van de AVG en de Wpg. Hoewel de taakstelling van de KMar verschillende vormen van gegevensverwerking in beginsel rechtvaardigt, leidt het samenbrengen van verschillende vormen van gegevensverwerking in het systeem tot onduidelijkheden met betrekking tot de doelbinding, noodzaak en evenredigheid. De huidige structuur maakt dat passagegegevens worden verzameld op grond van de AVG en structureel nader worden verwerkt op grond van de Wpg (vergelijking met kentekenlijsten).

Amigoboras is primair bedoeld ter ondersteuning van het MTV. Passagegegevens (kentekens) worden in beginsel verzameld om uitvoering te geven aan het MTV (inwinfunctie of selectiefunctie). Op grond van art. 4.17a Vreemdelingenbesluit is het MTV ingeperkt qua duur en frequentie. Passagegegevens (kentekens) worden met behulp van Amigoboras echter ongelimiteerd verzameld en nader verwerkt voor andere politietaken. Het valt te verdedigen dat de praktijk waarbij kentekens ongelimiteerd worden verzameld en nader worden verwerkt voor politietaken in strijd is met de beperkingen zoals opgenomen in art. 4.17a Vreemdelingenbesluit en bovendien in strijd is met de eisen van noodzakelijkheid en evenredigheid.

Het risico bestaat dat niet-gerechtigden kennis nemen van persoonsgegevens als gevolg van een datalek. De belangen van de kentekenhouder kunnen daardoor worden aangetast. Voor een betrokkenen kan het schadelijk zijn als passagegegevens in combinatie met profielen, kentekenlijsten, of een Quick Alerts met eventueel gevarenclassificaties voor niet-gerechtigden inzichtelijk zijn. Het is echter onwaarschijnlijk dat gegevens vanuit Amigoboras in handen komen van niet-gerechtigden, omdat er beveiligingsmaatregelen zijn getroffen op zowel technisch als organisatorisch vlak. Gevoelige gegevenselementen zijn middels codetabellen versluierd, waardoor de feitelijke betekenis voor buitenstaanders verborgen blijft. Als passagegegevens (verzamelde kentekens) uitlekken zal de impact naar verwachting gering zijn. Als politiegegevens uitlekken kan de impact hoog zijn.

Het sensordomein is in beheer bij een externe partij, namelijk **Art. 10 (2) (g)**. Beheerders van **Art. 10 (2) (g)** hebben in het kader van de beheerstaak toegang tot de door de camera's verwerkte gegevens. Concreet gaat het om **Art. 10 (2) (g)** het kenteken, het herkende kenteken aangevuld met RDW-gegevens en **Art. 10 (2) (c), Art. 10 (2) (d)**.

[REDACTED]. Met [REDACTED] is geen verwerkersovereenkomst afgesloten. Er is een risico dat via de gegevensverwerker data wordt gelekt of gemanipuleerd. De kans dat het risico zich voordoet is klein, gelet op de ABDO accreditatie van de gebruiker. De impact voor de kentekenhouder is naar verwachting gering.

Het is mogelijk dat gegevens van KMar-medewerkers en contactgegevens (verbonden aan kentekens) uitlekken. Het is niet waarschijnlijk dat deze gevolgen intreden. Als het risico werkelijkheid wordt, zal de impact naar verwachting gering zijn.

Van groot belang is dat de kwaliteit (integriteit) van de gegevensverwerking binnen Amigoboras voldoende is. Een onvoldoende werkend sensordomein betekent dat analyses niet de juiste kwaliteit hebben en onterechte acties kunnen worden uitgevoerd. Om dit risico te beperken kent het systeem grenswaarden. Bovendien vindt tijdens acties validatie plaats door KMar-medewerkers.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen



Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Onderstaande maatregelen zijn genomen om risico's ten aanzien van betrokken in te perken:

- Het Defensie Beveiligingsbeleid (DBB) is in acht genomen. De secretaris-generaal van het Ministerie van Defensie heeft middels de aanwijzing SG-003 het DBB vastgesteld. In deze aanwijzing zijn het algemeen beveiligingskader, de organisatie, taken en verantwoordelijkheden en de overlegstructuren beschreven. Daarnaast zijn de kaders opgenomen voor de deelgebieden van de integrale beveiliging. De deelgebieden omvatten de beveiliging algemeen en organisatie, personele beveiliging, fysieke beveiliging, informatiebeveiliging en industriebeveiliging. In de onderliggende DBB-instructies staan per deelgebied de normen waaraan moet worden voldaan om de onderkende (vitale) defensie belangen te beschermen. Het is in het belang van defensie om de rechten van de betrokkene van Amigoboras te waarborgen.
- De informatie die verwerkt wordt middels Amigoboras is vastgesteld op Te Beschermen Belang (TBB) niveau 3.¹⁵ Dit vormt de uitkomst van de VIR E&E risicoanalyse uit 2010.
- Om invulling te geven aan het beginsel 'privacy by design' is het systeem technisch zodanig ingericht dat het flexibel kan worden ingezet. Het systeem kan op onderscheiden locaties op verschillende manieren worden ingezet. Hierdoor wordt zo min mogelijk inbreuk gemaakt op de rechten van betrokkenen.
- Er is een ABDO-accreditatie voor **Art. 10 (2) (g)**, Cap Gemini en [REDACTED]
- Vanuit het beginsel van 'privacy by design' zijn gegevenselementen die een gevoelig karakter dragen, te weten gevarenclassificatie en profiel, versluierd. Door het gebruik van codetabellen is de feitelijke betekenis voor buitenstaanders verborgen. In geval van uitlekken blijft de schade gering.
- KMar-medewerkers en de beheerders van de Defensie Materieel Organisatie (DMO) zijn beëdigd en gescreend door de MIVD.
- Middels een autorisatiematrix wordt zeker gesteld dat alleen medewerkers toegang tot de Amigoboras hebben die het systeem nodig hebben voor hun werkzaamheden. Bovendien kent het systeem gelden verschillende rolgroepen.

Verbetermaatregelen

- Er is beleidsmatig niet vastgelegd hoe de processen/taken aan de binnengrenzen, waar Amigoboras ondersteunend aan is, ingevuld moeten worden. Het advies is dit uit te werken. Daarbij dient invulling gegeven te worden aan de discretionaire ruimte van art. 4.17a Vb.
- Het is aan te raden de systeemarchitectuur zodanig vorm te geven dat er een helder onderscheid is tussen gegevensverwerking op grond van de AVG en de Wpg.
- Het sensor domein van Amigoboras is in beheer bij een externe partij, namelijk [REDACTED]. Het ontbreekt echter aan een bewerkersovereenkomst. Geadviseerd wordt alsnog een bewerkersovereenkomst op te stellen.
- De VIR E&E risicoanalyse is opgesteld in 2010 en daarmee verouderd. Inmiddels ligt een nieuwe VIR E&E voor ter ondertekening door de DOPS-KMar.
- Digitale aanvraagformulieren met verzoeken om in het grensgebied naar kentekens te zoeken blijven in een functionele mailbox bewaard. Geadviseerd wordt dit proces nader te analyseren en een meer robuuste oplossing te realiseren waarbij de eisen vanuit de privacyregelgeving, zoals de bewaartermijn, gewaarborgd zijn.
- Hoewel het datawarehouse van de KMar buiten het bestek van deze PIA valt, wordt enerzijds geadviseerd een passende bewaartermijn vast te stellen voor gepseudonimiseerde gegevens en anderzijds zekerheden in te bouwen teneinde te voorkomen dat gepseudonimiseerde gegevens voor andere doeleinden worden gebruikt dan waarvoor verzameld.
- Logginggegevens van medewerkers blijven bestaan. Er is geen vernietigingsproces ingeregeld. Geadviseerd wordt bewaartermijnen vast te stellen en het vernietigen van deze gegevens te automatiseren.
- Rondom het gebruik van het Amigoboras systeem wordt gewerkt met de e-mail functionaliteit. Gebruikers kunnen mail verwijderen, maar de mail blijft in het archief bestaan. Geadviseerd wordt een alternatief te zoeken dat beter aansluit bij de privacyregelgeving.



Februari 2020



Inleiding

Uit informatie van Europol blijkt dat een Art. 10(2)(c) crimineel netwerk actief is in Nederland (onder de paraplu) van [redacted]. Zij worden ook wel [redacted] of [redacted] genoemd. In de publieke sfeer vertoont [redacted] zich als [redacted]. Het netwerk houdt zich internationaal via Art. 10(2)(c) bezig met handel in **verdovende middelen, witwassen**. Ook zijn er indicaties [redacted]. Het netwerk maakt veel gebruik van identificerende, karakteristieke, kenmerken en is sterk georganiseerd (zie bijlage).

Verdieping

Nederland blijkt een Art. 10(2)(c) schakel te zijn in het netwerk. [redacted] het netwerk zijn in Nederland actief om drugs naar [redacted] ([redacted] en [redacted]) te smokkelen. Voor zover bekend gaat het om smokkel van [redacted] en [redacted]. Eigenaarschap van de drugs blijft in Nederland totdat de drugs is verkocht. De omzet vloeit terug naar [redacted]. Hierbij wordt gebruik gemaakt van [redacted] koeriers die afhankelijk worden gemaakt door Art. 10(2)(c) [redacted]. De winst wordt vervolgens naar [redacted] getransporteerd en wordt witgewassen via

Art. 10(2)(c)

Art. 10(2)(c) organisaties. Hierbij wordt geïnvesteerd in [redacted] en [redacted] in [redacted]. Leden hebben allemaal de [redacted] nationaliteit en worden daar geworven. Er zijn echter nauwelijks [redacted] personen betrokken in de 'eerste lijn' (drugsverkoop op straat etc.) in Europa, dit zijn vooral andere [redacted] migranten die hier worden gerekruteerd.

Subjecten uit het netwerk zijn moeilijk detecteerbaar door Art. 10(2)(c) [redacted]. Rekrutering van leden gebeurt met behulp van [redacted] [redacted]

[redacted]. Ook zijn hierbij indicaties Art. 10(2)(c) [redacted]. Het netwerk is zeer gewelddadig. Daarbij hebben ze toegang tot [redacted]. Indien het noodzakelijk wordt geacht zal het netwerk samenwerken met andere [redacted] organisaties en/of gebruik maken van Art. 10(2)(c) [redacted] facilitators.

Uit lopende onderzoeken blijkt dat Art. 10(2)(c) [redacted] reisroutes worden gebruikt [redacted]. Er zijn casussen bekend waarbij drugs via [redacted] Nederland verlaat maar ook [redacted] worden genoemd. Ook reisbewegingen van/naar Art. 10(2)(c) [redacted] komen uit de informatie naar voren. Over [redacted] routes en de [redacted] geldstroom is [redacted] bekend.

Mogelijk relevante trends en ontwikkelingen binnen KMar-domein

Gezien bovenstaande bevindingen en het uitgebreide KMar-domein bestaat de mogelijkheid dat de KMar operaties met dit criminele netwerk in aanraking komt. Ondanks dat concrete casussen ontbreken zijn er verschillende trends en ontwikkelingen relevant waarbij bovenstaande informatie als achtergrondinformatie van meerwaarde kan zijn. In onderstaande beschreven trends en ontwikkelingen is voortsnog geen link vastgesteld met Art. 10(2)(c) [redacted]

Al enige tijd wordt gewezen op de hoge instroom van Art. 10(2)(c) [redacted] vreemdelingen naar Nederland. Sinds ingang [redacted] in augustus om de instroom te beperken is sprake van een daling van het aantal [redacted] vreemdelingen; echter, de instroom is zeker niet opgedroogd en [redacted] blijven terugkomen in de top [redacted] instroom IND. Aandacht blijft dan ook geboden voor [redacted] migratie van [redacted] vreemdelingen.

Vanuit registraties en onderkende Incidenten vooral aandacht aan de [redacted] grens per Art. 10 (2) (c) [redacted], o.a. [redacted].¹

Op de grensprocessen op de luchthavens is zichtbaar dat er [redacted] Art. 10 (2) (c) vreemdelingen zijn geweigerd in de achterliggende maanden, ook het aantal asielaanvragen op de luchthavens was [redacted].²

Er zijn binnen de huidige beschikbare informatie geen concrete verbanden te leggen maar opvallend is dat naast de indicaties van [redacted] Art. 10 (2) (c) bij Art. 10 (2) [redacted] er ook enkele opvallendheden te noemen zijn op het gebied van [redacted] in relatie tot de [redacted] nationaliteit:

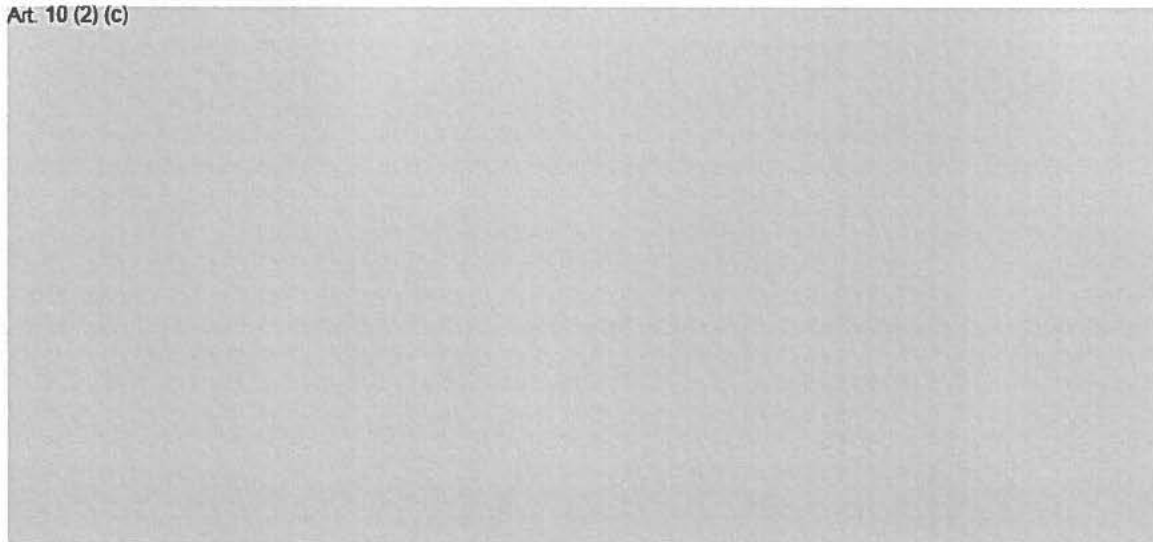
Er zijn in de afgelopen periode signalen binnengekomen vanuit verschillende asielzoekerscentra m.b.t. het verdwijnen van Art. 10 (2) (c) asielzoeksters met onbekende bestemming. De vrouwen zijn vaak [redacted] via [redacted] Europa binnengekomen. De [redacted] vrouwen zijn vervolgens naar Nederland gereisd [redacted], waarbij het verhaal is dat [redacted]. De vrouwen vragen vervolgens asiel aan. [redacted] verdwijnen de vrouwen uit de opvang [redacted].³ Dit zou mogelijk een signaal van [redacted] kunnen zijn. [redacted] Op dit moment is [redacted] om [redacted] verbanden te onderkennen.⁴

Aandacht OPS

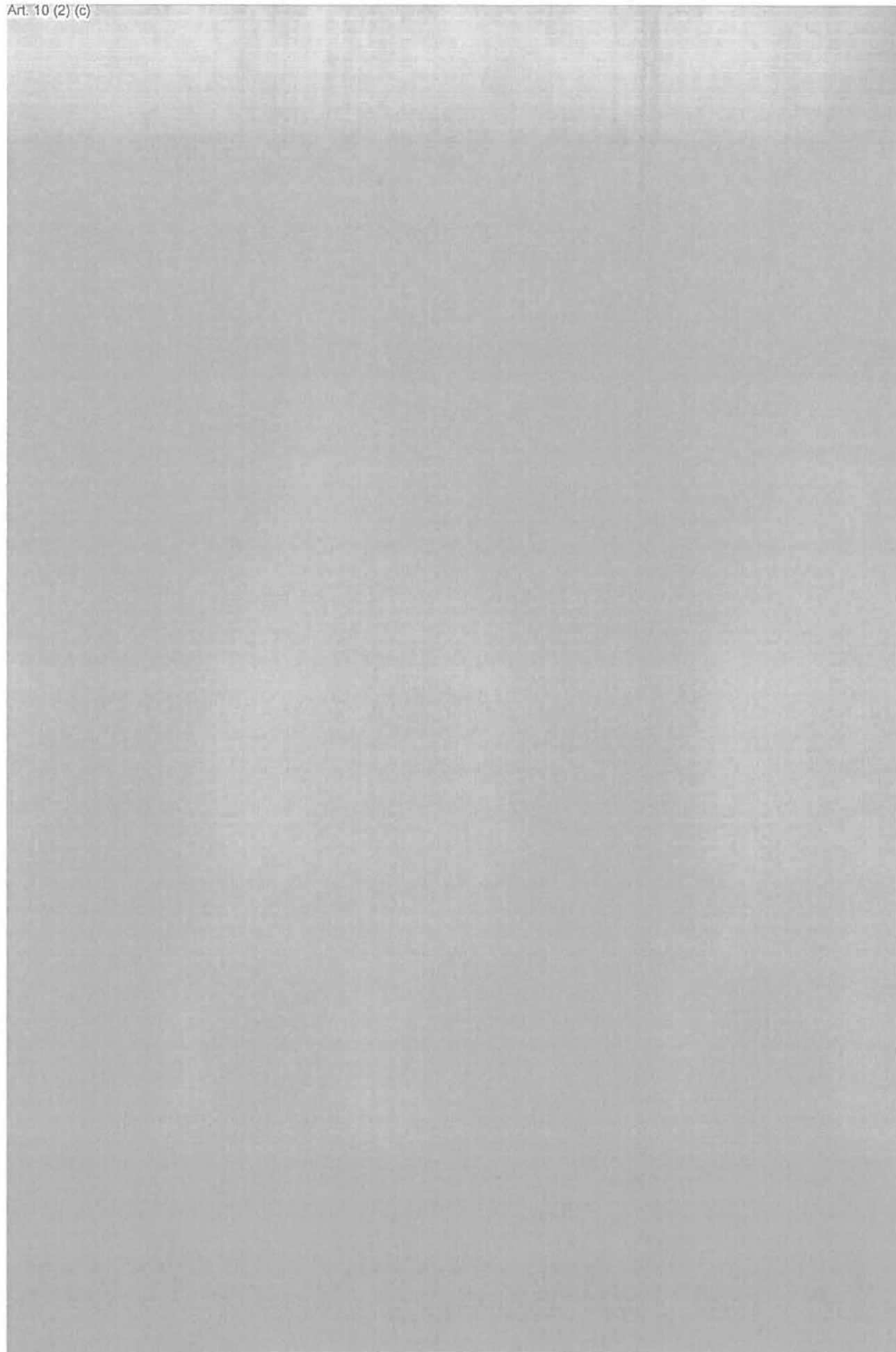
- Heb bij casussen binnen de operatie aandacht voor georganiseerdheid zoals in dit product beschreven;
- Muteer bij aantreffen van Art. 10 (2) (c) [redacted] kenmerken en/of andere signalen van aanwezigheid van [redacted] zo uitgebreid mogelijk de onderkende bevindingen;
- Deel relevante bevindingen op het gebied van [redacted] altijd ook via d [redacted]
- Wees alert op [redacted] van criminaliteitsvormen [redacted] bij mogelijk gerelateerde casussen ([redacted])

Identificerende, karakteristieke, kenmerken [redacted]

Art. 10 (2) (c)



Art. 10 (2) (c)





OPENBAAR MINISTERIE

Kwaliteitskader Big Data

OM en Politie

Programma Toekomstbestendig Opsporen en Vervolgen

Extern

Versie 1.0

Versie datum: 11 mei 2020

Status: Versie voor eerste implementatie

« waakzaam en dienstbaar »

Inhoudsopgave

Inhoudsopgave	2
Maatschappelijke vraagstukken en achtergrond bij het Kwaliteitskader Big Data	3
Kwaliteitskader	3
Checkvragen kwaliteitskader	5

Maatschappelijke vraagstukken en achtergrond bij het Kwaliteitskader Big Data

Het gebruik van kennistechnologie, met in het bijzonder het gebruik van algoritmen, data analysemethoden en Big Data (en daarmee 'Big Data-technologie') voor effectievere opsporing en vervolging brengt maatschappelijke, juridische en ethische vraagstukken en dilemma's met zich mee. Het inventariseren, het doen beantwoorden van deze vragen en het kaderstellend maken van de antwoorden voor andere Big Data-initiatieven is van belang om betrouwbare analyse-instrumenten te ontwikkelen of aan te kopen om zodoende te resulteren in betrouwbare informatie.

Het Wetboek van Strafvordering en de Politiewet geven de voorschriften voor het verzamelen van gegevens. De Wet politiegegevens geeft de voorschriften voor het verwerken van deze gegevens voor zover het politiegegevens betreft. Het uitgangspunt is dat het gebruik van Big Data-technologie altijd is gebaseerd op rechtmatig verkregen, verwerkte en gecombineerde informatie. De verwerking en analyse van gegevens (automatisch of handmatig) is controleerbaar, reproduceerbaar en kritisch toetsbaar. Algoritmen en modelparameters die voor bijvoorbeeld risicotaxatie en toekomstverwachtingen worden gebruikt zijn bekend, wetenschappelijk getoetst en controleerbaar (inzichtelijk en transparant). Een belangrijk uitgangspunt is dat altijd wordt voldaan aan de wet en dat dit ook inzichtelijk is. Het Openbaar Ministerie (OM) en de politie nemen, na de beantwoording van (de vragen in) het kwaliteitskader en het geschetste plan van aanpak van het Big Data initiatief of project, gezamenlijk een moreel standpunt in over het gebruik en de inzetbaarheid van de technologie en de daaruit voortvloeiende informatie.

Kwaliteitskader

Dit kwaliteitskader is een product van het programma Toekomstbestendig Opsporen en Vervolgen, opgesteld in nauwe samenwerking tussen Politie en OM. De opzet van dit kwaliteitskader is meerledig. De benaming Kwaliteitskader Big Data is specifiek gekozen omdat dit kader verschillende doelen dient. Het is zowel een beschrijvings- als een toetsingskader. Het is geen voorschrijvend kader of 'control framework'. Het kader wil op een methodologische wijze vooral inzichtelijk maken hoe een Big Data project of activiteit is opgezet, wordt uitgevoerd en welke 'checks and balances' aanwezig zijn. Het creëren van bewustzijn in de uitvoering is een belangrijk aspect om daar waar nodig ook (al dan niet mitigerende) maatregelen te kunnen nemen. In de opzet van het kader wordt op hoofdlijnen de stappen gevolgd zoals in de methode CRISP-DM¹ zijn beschreven, aangevuld en gemengd met specifieke vragen geënt op juridische, maatschappelijke en ethische aspecten welke voortkomen uit geldende wet- en regelgeving alsmede belangrijk te beschermen normen en waarden. Hierbij moet worden aangetekend dat de te stellen vragen niet uitputtend en limitatief zijn en er geen goede of foute antwoorden zijn. Verder is het van belang om de beantwoording van de vragen in de vorm van een interview met betrokkenen uit te voeren en te doorlopen waardoor een gedegen risico-inschatting en plan van aanpak kan worden geformuleerd.

Het kader kent geen harde (cijfermatige) normen waar tegen gemeten kan worden, het maakt eventueel aanwezige risico's wel inzichtelijk. Hiermee is het geschikt om als hulpmiddel in te zetten bij risico-inschatting en toetsing, waaronder een toetsing door een Officier van Justitie (OvJ) vanuit het OM. Dit is specifiek van toepassing wanneer er sprake is van een directe relatie naar de opsporing. Op basis van de verkregen inzichten kan vervolgens worden gehandeld. Daarbij kan het gebruikt worden om een Gegevensbeschermingseffectbeoordeling (GEB) op te stellen. Of dit noodzakelijk is blijkt uit een pre-GEB. De vragen uit het Kwaliteitskader komen overeen met die van de pre-GEB.

¹ CRISP-DM staat voor Cross-industry standard process for data mining. Dit is een open standaard procesmodel wat sinds 1996 in gebruik is en wereldwijd tot op heden het meest gehanteerde model voor data mining. De keuze voor CRISP-DM als basis voor het kwaliteitskader is mede gebaseerd op het gebruik van deze methode binnen de politie voor Data Science projecten.

Officieren van justitie willen kunnen toetsen/sturen op het moment dat een Big Data project wordt gestart in de pre-opsporingsfase (lees: intelligence fase), binnen bestaande opsporingsonderzoeken of opsporingsonderzoek overstijgend. Dit is afhankelijk van de werking en toepasbaarheid van de te ontwikkelen of in te zetten technologie. Dit alles zodat in de vervolgingsfase geen risico's ontstaan als het gaat om de herkomst van data, kwaliteit van data, bevoegdheid of betrouwbaarheid van toegepaste analysemethoden of gebruikte systemen. Wat wel of niet goed is willen we tot uiting brengen via het kwaliteitskader waarbij we de overwegingspunten inzichtelijk maken. Daarmee is het kader geen methode om specifiek en expliciet inzicht te krijgen in de algoritmes zelf, zoals bijvoorbeeld de integriteit, uitlegbaarheid en redelijkheid van het algoritme. De Politie en OM willen door middel van het kwaliteitskader inzicht verkrijgen om een zo goed mogelijke en proportionele afweging te kunnen maken. De OvJ kan een toetsende rol hebben als het gaat om het aangeven van deze grens.

Dit kwaliteitskader is een 'levend' document. Het gebruik in de praktijk zal wijzigingen opleveren om dit kader verder te verbeteren. Daarbij zal o.a. ook worden gekeken naar ontwikkelingen m.b.t. het gebruik van data en literatuur over verantwoord gebruik van Data Science. Ook de zeer snelle ontwikkelingen in technologie hebben invloed op de verdere ontwikkeling. Het kwaliteitskader is de afgelopen tijd met veel zorgvuldigheid opgesteld en is in lijn met nationale en internationale ontwikkelingen op het gebied van kaders en richtlijnen in dit verband. Momenteel zijn Politie en OM in beide organisaties bezig met de implementatie en inbedding van het kwaliteitskader. De implementatie ziet op opleiding, organisatorische en technische inbedding.

Checkvragen kwaliteitskader

Fase	Vraag	Toelichting vraag	Zwaartepunt te beschermen waarden
Fase 0 – Titel plan/aanpak	Hoe zou je jullie aanpak / voorgenomen plan willen omschrijven? Wat is de naam van de aanpak / het plan?	T.b.v. de herkenbaarheid van het projectplan en de eerste potentiële doelbeschrijving.	Communicatie, transparantie, vertrouwen, taakgetrouwheid als uitvoerende organisatie in een rechtsstaat
Fase 1a – Inzicht bedrijfsdoelstelling (algemeen)	- Wat is het doel van het voornemen/ big data traject? - Welk probleem wil je oplossen met behulp van data? - Wie is de opdrachtgever/ verantwoordelijke? - Welke andere partners zijn betrokken? - Is het (eind)doel om inzicht in data te verkrijgen of om een model te ontwikkelen? - Welk soort beslissingen wil je ermee nemen (operationeel, tactisch of strategisch)? - Achtergrond van het plan/idee/werk (eerdere ervaringen, gebruik in buitenland, op de oude manier ging het niet, beleidsuitvoering, omdat het kan, nieuwe werkvormen uitproberen,...)? - Zijn er KPI's benoemd? Expliciet of impliciet? - Wanneer is het plan/idee tot een succes te benoemen? Welk probleem ga je hiermee oplossen? - Met welke dataset/ type data zou je dit plan/idee willen oplossen? Verwerk je bijzondere persoonsgegevens of gegevens van kwetsbare personen (minderjarigen, vluchtelingen, etc.)? Wat is de onderbouwing hiervan? (NB: hier wordt in fase 2 uitgebreid op ingegaan).	- Vooraf relevant bij de toepassing van nieuwe technologieën die risico's kunnen opleveren in de strafzaak. Denk aan voorspellende en voorschrijvende analyse vormen. - Enorm belangrijke fase aangezien dit de meetlat vormt voor de in te zetten databronnen/ te hanteren technieken etc. - Dwingt juridisch gezien tot doel bepaling en tot kritische beschouwing datagebruik. - Dwingt om kritisch te kijken naar de grenzen van artikel 3 Politiewet en aanpalende wetgeving waar Politie bevoegdheid uit ontleent. - Kijkend naar de laatste vraag van dit blok kan het qua risico-inschatting uitmaken of een project direct in de operatie wordt ingezet of dat het in de R&D omgeving blijft voor nader onderzoek >> ruimte voor innovatie. Bij de inzet van nieuwe technologieën met een risico voor de rechten van betrokkenen is een GEB verplicht en als de maatregelen niet toereikend zijn de AP moet worden ingelicht. Vraag is relevant voor de pre-GEB. - Deze en de voorgaande vraag zijn relevant in het kader van een pre-GEB.	Veiligheid en toetsing van het systeem, gelijkheid (fairness), privacybescherming, transparantie, vertrouwen, taakgetrouwheid als uitvoerende organisatie in een rechtsstaat

	• Is er een voornemen om een prognose of een voorspelling te doen op basis persoonskenmerken (profilering)? • Binnen welke onderzoeksfase wordt het project/plan gestart? (intelligence/opsporing/vervolgning)? • Op basis van welke politieke grondslag (politiewet/politietak) wordt dit doel gerealiseerd? • Wat is de scope van het project en wat ga je nu afbakenen in relatie tot het doel? • Gaat er gebruik gemaakt worden van een 'innovation space' tussen TRL fases en eventueel een 'safe harbor' of experimenteertomgeving? • Op welke wijze wordt het resultaat van het project gebruikt? Wordt het in de operatie (kan gaan om alle fases van onderzoek, de intelligence fase en de opsporingsfase) geïmplementeerd? • Betreft het een nieuwe technologische methode, waarbij persoonsgegevens worden verwerkt? Of betreft het de verbetering van bestaande analyse toepassingen/systemen?	• Breng verwachtingen helder in kaart. • Let op een eventuele 'scope creep' (ongecontroleerde wijzigingen in de oorspronkelijk opzet).	
Fase 1b – Inzicht bedrijfsdoelstelling (methode)	• Welke vorm van analyse of analytics beoog je te gebruiken? Beschrijvend, verklarend, voorspellend of voorschrijvend? • Ligt er een hypothese aan de doelstelling ten grondslag? • Is deze hypothese gestaafd met operationele feiten en kennis en/of ook wetenschappelijk? Graag uitvoerige toelichting. • Zijn er naast data scientists ook materiedeskundigen betrokken bij het project?	• Deze vragen dienen om te voorkomen dat er wordt gedaan aan een 'fishing expedition' en dwingt tot kritische reflectie op de inzet van de methodieken in relatie tot de initiële scope onder fase 1a. • Ook dit draagt bij aan uitlegbaarheid van de analyse. Het behoeft geen uitleg dat wetenschappelijke validatie sterk de voorkeur heeft. • Domeindeskundigheid is cruciaal.	Controle over de technologie, inclusiviteit, gelijkheid, autonomie, voorkomen willekeur, balans machtsverhoudingen (rechtszekerheid in taakuitvoering)

	Denk aan criminologen of psychologen. Welke materiedeskundigen zijn betrokken en waarom denk je deze specifieke competenties nodig te hebben? • Welke experimenten zou je moeten doen om de hypothese te valideren? • In hoeverre is het instrument een direct of indirect sturend instrument, wie beslist wat en wat betekent dit voor de operationele inzet? • Welke vastleggingen ga je doen tijdens de uitvoering van het te doorlopen traject?	• Validatie is van groot belang. Kun je hypothesen valideren door nieuwe experimenten te doen > validatie experiment > nieuwe data of data zoeken. • Let op. Niet elke "(domein)expert" is daadwerkelijk een expert het gebied van data science. Goed identificeren > houd de combinatie met het echte veldwerk! • Betrekken van materiedeskundigen heeft sterk de voorkeur in een project aangezien data scientists alleen niet voldoende zijn gezien beperkte kennis van de operatie/ het kennis gebied. Het is van groot belang dat materiedeskundigen evenals privacy deskundigen al aan de tekentafel betrokken worden. Het streven is met een multidisciplinair team te werken aan een plan van aanpak. • Laatste vraag zit op de functie van het instrument in de operationele fase. Hoeveel impact heeft het instrument in de operatie en beoog je dit ook?	
Fase 1c – Inzicht bedrijfsdoelstelling (risico's)	• Zijn er risico's op maatschappelijk/ethisch of juridisch gebied? Zo ja wat zijn de mitigerende maatregelen? Zijn er eventueel ook nog andere risico's? • Wordt er gebruik gemaakt van gegevens waar een machtiging voor moet worden gegeven? • Kan de in te zetten of te ontwikkelen technologie gekwalificeerd worden als een BOB-middel? > denk aan OSINT tooling of vergaande profile ontwikkeling tussen datasets of sensing,	• Meestal gaat het over bijzondere persoonsgegevens wanneer men beoogt om bijvoorbeeld sensing technologie te ontwikkelen of data in te zetten. Met deze vragen kunnen we risico's als het gaat om projecten waar vanuit het bevoegd gezag goedkeuring/ machtiging voor afgegeven had moeten worden. • Het gaat hierbij ook om stelselmatige en grootschalige monitoring. Deze vraag is relevant in het kader van de pre-GEB. • Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn (in combinatie verwerken	Voorkomen van discriminatie, autonomie, inclusiviteit, privacy, transparantie, gelijkheid, voorkomen detournement de pouvoir, controle over data bescherming

	• Worden er datasets gecombineerd die voortkomen uit gegevensverwerkingen met verschillende doelen? • Wordt het landelijk vastgestelde autorisatiemodel gevolgd? Zo nee; wat is hiervoor de reden? Wie heeft daar mee ingestemd? en zo nee waarom niet? Zijn er problemen te voorzien wanneer mensen niet de toegang krijgen tot gegevens waar zij formeel (rol gebaseerd) toegang toe hebben? Leidt dit bijvoorbeeld tot uitkomsten die disproportioneel zijn? • Op welke wijze wordt er gecontroleerd dat er aan het landelijk autorisatiemodel van de politie wordt voldaan? Wordt dit bijvoorbeeld gelogd of op een andere wijze? • Is de autorisatie anders bij de ontwikkeling van het project versus het gebruik van het eindresultaat?	heet dat nu in de Wpg) waarvan de betrokkene dat redelijkerwijs niet zou verwachten (vraag uit pre-GEB). • Het autorisatiemodel is vastgesteld door zowel politie als OM. Dus noodzaak om hier van af te wijken moet serieus worden onderbouwd. Wil je hier van afwijken dan is er een handmatige procedure maar dat moet wel in overleg met de teamchefs (is bestaand proces voor ingericht). In de eigen beheerde omgevingen of omgevingen waarop de technologie wordt ontwikkeld of gedraaid wordt de autorisatie gebruikt vanuit functie en rol. Dit is soms lastig omdat je in een protocol soms minder mag. Eveneens dient dit gecontroleerd te worden vanuit logging. • Toelichting op laatste vraag: ontwikkelaars hebben andere autorisaties dan eindgebruikers > dit dient goed uit elkaar gehouden te worden in het plan van aanpak en de uiteindelijke uitrol. Bij de autorisatie wellicht kijken naar logging. Wat je zou kunnen beperken aan de output kant > dat de Data Scientist er niet verder mee mag en kan. Een optie is een scheiding tussen sec het Data Science werk (ontwikkelen) versus het in de praktijk gaan testen en gebruiken. Denkrichting voor een extra waarborg. Je kunt dan vrijheid geven voor de verbinding en anderen het vervolg laten oppakken.	
Fase 1d – Inzicht bedrijfsdoelstelling ((externe) tooling)	• Van welke tools en technieken wordt er gebruik gemaakt? Wordt er gebruik gemaakt van Open Source code / software? Zo ja, hebben we ook inzicht in de aard van deze data	• Deze vragen zijn voornamelijk bedoeld om tegemoet te komen aan het principe van transparantie en uitlegbaarheid in de rechtszaal. Indien sprake is van een NDA betekent dit dat we niet kunnen komen tot	Vertrouwen in technologie, controle over technologie, transparantie, gelijkheid, controle op algoritme, voorkomen detournement de pouvoir,

	waarop is getraind en de gehanteerde parameters? • Wordt het werk/plan vormgegeven in samenwerking met een commerciële/ externe partij? En zo ja, welke • Wordt er gebruik gemaakt van data aangeleverd door externe/ commerciële partijen ofwel direct ofwel indirect voor de training van een algoritme? • Is er voldoende inzicht in de verkrijging van de data ook indien dit door een commerciële of externe partij is vergaard? Op welke wijze is dit gevalideerd? • Heeft de externe/commerciële partij een NDA afgekondigd waardoor je onvoldoende inzicht hebt in de werking van het product of er wordt opgelegd dat politie/OM als contractspartij in de rechtszaal niet kunt spreken over de totstandkoming van het product? • Zijn er afspraken gemaakt met de commerciële of externe partij over het eigenaarschap van de data met deze commerciële partij? • Is er volledig zicht op de werkzaamheid van het algoritme?	volledige transparantie kijkend naar bepaalde conclusies. Uiteraard is de beantwoording van deze vraag wel afhankelijk van het type Big Data project. • Let op >> in toekomst is de verwachting dat in toenemende mate gebruik wordt gemaakt van "off the shelf" algoritmes. Deze algoritmen zitten soms al in commerciële tools of kunnen openbaar door Data Scientist worden gedownload. Daardoor kan transparantie van algoritmen lastiger worden. • Zou bepaalde tooling aan onafhankelijke keuring onderworpen kunnen worden als er een grote maatschappelijke impact is te verwachten? • Is het mogelijk om een tool in te zetten voor de validatie van de eerste "hunch" (zit je in de goede richting of heb je een redelijk vermoeden) > daarna helemaal valideren en afpellen tot de kern > context discovery verkennen>> Op welke wijze kun je dit vertrouwen in het project vergroten?	machtsverhoudingen (rechtszekerheid in taakuitvoering), voorkomen van willekeur, vrijheid van meningsuiting, informatieveiligheid
Fase 1 Inzicht bedrijfsdoelstelling (afsluitende vraag fase 1)	• Zijn er – als het gaat om de het inzicht in de bedrijfsdoelstelling - nog andere onderwerpen die je ter sprake wilt brengen? • Hebben de inzichten na de beantwoording van dit eerste blok geleidt tot andere ideeën of inzichten? Is het noodzakelijk om de bedrijfsdoelstelling hierop aan te passen?	• Indien wordt gesignaleerd dat aanpassing in eerdere fase noodzakelijk is dienen alle vragen wederom doorlopen te worden.	Controleerbaarheid van het systeem, transparantie, validiteit
Fase 2a – Inzicht data (bron)	• Wat is de bron van de data set? Wat is de methode van data verzameling geweest? Bijvoorbeeld interne politie data//BD/OSINT	• Denk hierbij aan bronnen als SumMIT, OSINT, BVH, KvK, GBA etc.	Validiteit, controleerbaarheid, transparantie, voorkomen censuur, inclusiviteit, privacy,

	etc. Of wat zijn de bronnen van de commerciële of derde partij? • In hoeverre ben je gaan 'grasduinen' door de data om er een goed begrip van te krijgen? • Heb je een volledig begrip van de data die je beoogde te gaan gebruiken of zitten er onbekende elementen in? Zo ja, hoe wil je daar mee omgaan? • Wat is de overweging geweest om de geselecteerde data te kiezen? • Is overwogen om ook synthetische data te gebruiken (bijvoorbeeld door het ontbreken van data of om een grotere hoeveelheid beschikbaar te hebben)? • Wat is de juridische grondslag om van deze bron data te verkrijgen? • Indien politiedata wordt gebruikt; welke Wpg verwerkingscategorie gebruik je? 8/9/10 Wpg of bijzondere wetgeving. • Gebruik je informatie welke niet direct onder het regime van de Wpg valt? Bijvoorbeeld OSINT informatie. • Is er toestemming voor het gebruik van de gegevens nodig door degene die deze heeft verzameld? Vooral aan de orde bij samenwerkingen met derde of commerciële partijen. • Is het nodig om degene die de data van oorsprong heeft verzameld te informeren over het gebruik ervan? • Op welke wijze wordt er rekening gehouden met de wettelijke bewaartermijnen van de te gebruiken datasets? Hoe heb je deze	• De OSINT vraag is expliciet opgenomen aangezien in veel gevallen nog de overtuiging is dat OSINT data per definitie gebruikt kan worden. Het tegendeel is natuurlijk geval gezien de huidige discussies in het licht van Modernisering Wetboek Sv en BOB middelen. • Er zijn ook algoritmes inzetbaar om de kwaliteit van de data te versterken (cleansing) > breed kijken naar de totstandkoming van de gebruikte data. • Dit kan bewerkstelligt worden door een veelvoud aan peer reviews. Het is belangrijk dat bij elke stap in het proces er bewustwording op het risico van bias aanwezig is. • Je zou een kennisgroep kunnen creëren die boven de partijen gaat staan> een multidisciplinair gebruikerspanel. OP deze manier kan geborgd dat verschillende achtergronden kijken naar de data en manier van data verwerving. • M.b.t. het gebruik van data t.b.v. het projectdoel: Zo kun je bijvoorbeeld niet in alle fasen van onderzoek gebruik maken van alle functies van de KvK en is artikel 10 en/of 9 info alleen toegankelijk onder bepaalde omstandigheden. • Probeer de eventuele fouten van andere partijen betrokken bij de ontwikkeling van externe tooling of de samenstelling van de te analyseren of trainingsdata goed inzichtelijk te krijgen.	informatieveiligheid, databescherming, vrijheid van meningsuiting, machtsverhoudingen (rechtszekerheid in taakuitvoering)
--	---	---	--

	waarborgen geïmplementeerd in je project/plan? • Zijn er door de eigenaar van de data of door andere betrokkenen verder voorwaarden gesteld aan het gebruik van de data of de resultaten die uit de analyse volgen? • Op welke wijze is er getoetst of beoogde data voor het genoemde projectdoel gebruikt kan worden?		
Fase 2b – Inzicht data (assess & ingest)	• Wat vind je van de kwaliteit van de data? • Welke vervuiling zou er in de data kunnen zitten? > denk aan notatie vormen, verkeerde invulvelden of vooringenomen/biased entries, (bijvoorbeeld aangiftebereidheid kijkend naar specifieke regio)? • Is er mogelijk sprake van unfairness in de data? • Is het nodig om de kwaliteit van de data te verbeteren voordat verder wordt gegaan? Hoe gaat dat worden gedaan? • Is er sprake van foutmarges in de data en hoe ga je daar mee om? • Zijn er aanwijzingen dat de dataset biased of vertekend is, bijvoorbeeld selectie bias in de datasets die als basis zijn gebruikt. Is het nodig om deze te verminderen? Hoe ga je dat doen? • Leidt deze fase tot andere inzichten in de business/ tot aanpassing van het doel? • Zijn de inhoudsdeskundigen ook betrokken bij het valideren van de kwaliteit van de data?	• Notatie/ entry velden zijn niet altijd gelijk waardoor het lastig is om de kwaliteit van de dataset te waarborgen. Dit is vooral van toepassing in BVH. Op welke wijze ondervang je dit in het project? • Dit probleem kan zelfs blijven ontstaan nadat de BI&K afdeling erdoorheen gaat. • Welke checks en balances worden tijdens analyse of ontwikkeling ingebouwd of op welke wijze is er achteraf sprake van validatie van de resultaten. Op welke wijze wordt achteraf rekening gehouden met de bias die ook daar aanwezig kan zijn voordat er conclusies worden verbonden aan de uitkomst? • Hoe ga je dit integer gebruiken, denk ook aan de inzet van een divers gebruikerspanel.	Vertrouwen, gelijkheid, privacy, autonomie, transparantie, inclusiviteit, voorkomen discriminatie, voorkomen censuur
Fase 2 – Inzicht data (afsluitende vraag fase 2)	• Zijn er nog andere onderwerpen die men ter sprake wenst te laten komen? Heeft men iets geleerd waardoor aanpassing in de bedrijfsdoelstelling noodzakelijk is?	• Indien wordt gesignaleerd dat aanpassing in eerdere fase noodzakelijk is dienen alle vragen wederom doorlopen te worden.	Controleerbaarheid van het systeem, transparantie, validiteit

Fase 3 – Preparatie data	• Is het nodig om persoonsgegevens te verwerken of kan het gewenste resultaat worden bereikt met geanonimiseerde / gepseudonimiseerde gegevens? • Als er bijzondere persoonsgegevens worden verwerkt, worden deze gegevens ingezet om bias tegen te gaan in het te ontwikkelen project? Kun je omschrijven welke eventueel extra waarborgen in acht zijn genomen om deze persoonsgegevens te beschermen? • Zijn de condities waaronder pseudonimisering opgeheven kan worden vooraf bekend? Hoe is dit geregeld? Bijvoorbeeld bij een derde partij? Is dit vastgelegd? • Op welke manier wordt de data gereed gemaakt voor analyse? En in hoeverre wordt dit vastgelegd? • Welke bewerkingen worden er uitgevoerd op de (ruwe) data om deze geschikt te maken voor gebruik? (denk bijvoorbeeld aan crunchen en combineren, patronen of anomalieën ontdekken) • Zijn de keuzes bij het gereedmaken, wijzigen of verwijderen van de data (onderdelen) vastgelegd? • Als geanonimiseerde data uit verschillende bronnen worden gecombineerd, is er dan een risico dat alsnog personen kunnen worden geïdentificeerd? Is dit risico geaccepteerd? Wat is de actie als het in werkelijkheid gebeurt.	• Beoordeel in hoeverre het daadwerkelijk nodig is om data weg te laten. Een goed algoritme maken is belangrijker dan data limiteren. • Train algoritmes op zo compleet mogelijke sets aan data • Controleer in hoeverre deelsets aan data bias opleveren. • Het gebruik van (bijzondere) persoonsgegevens moet goed worden afgewogen. Dit kan het geval zijn voor (alleen) het optimaal trainen van een model maar ook om het in de praktijk te kunnen gebruiken.	Privacy, gelijkheid, inclusiviteit, autonomie, transparantie, databescherming, voorkomen willekeur, validiteit, menselijke waardigheid
Fase 3 – Preparatie data (afsluitende vraag fase 3)	• Zijn er nog andere onderwerpen die men ter sprake wenst te laten komen? Heeft men iets geleerd waardoor aanpassing in de bedrijfsdoelstelling noodzakelijk is?	• Indien wordt gesignaleerd dat aanpassing in eerdere fase noodzakelijk is dienen alle vragen wederom doorlopen te worden.	Controleerbaarheid van het systeem, transparantie, validiteit

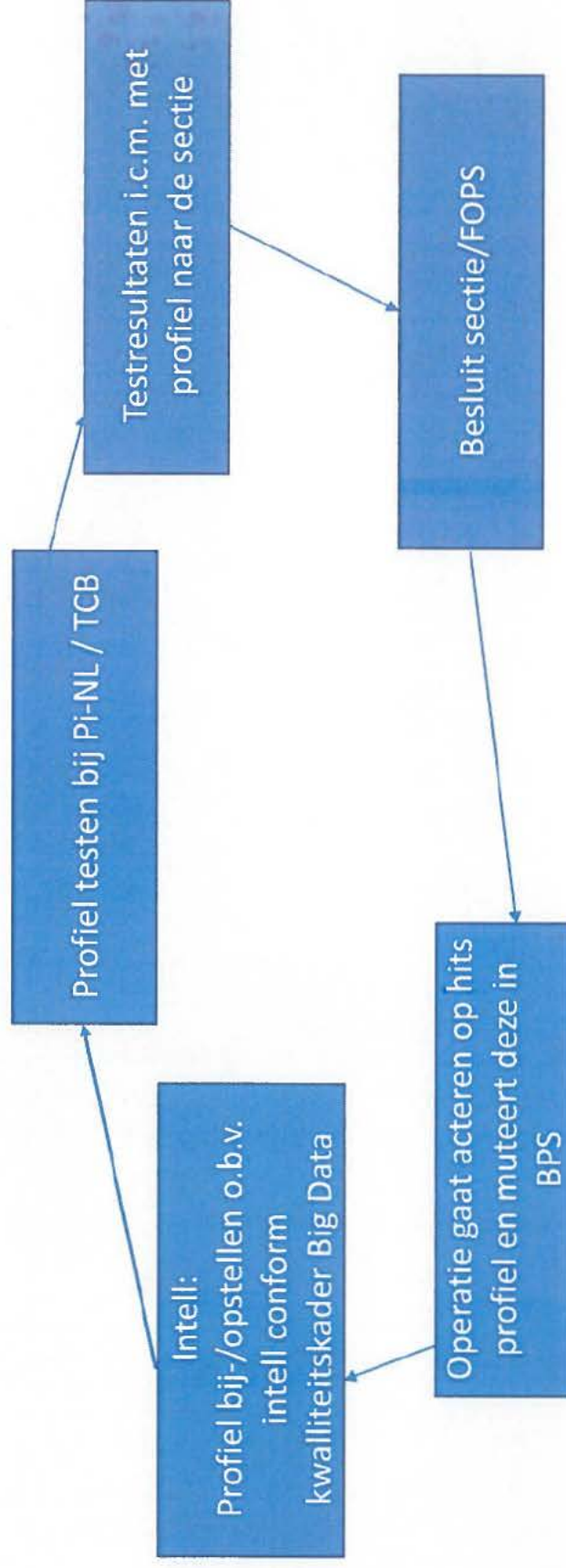
Fase 4 – Modelrealisatie	• Op welke wijze zijn de statistische modelleringstechnieken gekozen en zijn deze vastgelegd? Zijn deze gevalideerd en zo ja, hoe is dit gedaan? Er kunnen ook meerdere technieken naast elkaar gebruikt worden juist om de validiteit te verhogen. • Op welke wijze is het toegepaste model (ook indien commercieel aangeschaft) getraind? • Is er een plan voor trainen, testen en evalueren van het model? • Wordt er gebruik gemaakt van separate trainingsets en testsets? In hoeverre zijn deze sets random gesplitst? • Hoe werkt het model, is er een beschrijving aanwezig van de gehanteerde features en de betekenis? • Welke foutmarge is (situatie afhankelijk) is acceptabel voor gebruik in de praktijk en ben je in staat deze goed te interpreteren? • Op welke wijze (=hoe) is dit model/ het profiel/ AI gevalideerd? Welke statistische principes zijn hierbij gehanteerd? • Wanneer er gebruik gemaakt wordt van Deep Learning Netwerken, wat zijn de achterliggende overwegingen om voor een specifiek netwerk te kiezen (zoals RNN, CNN etc.)? • Is er gekozen voor een bepaald modelleringsdesign? Bijvoorbeeld kruisvalidatie, afzonderlijke trainingsmodellen. • Is het uiteindelijk gekozen model beschreven: ○ Wat gaat er in aan data?	• Let op: Indien nieuwe data in beeld komt is het noodzakelijk de voorgaande stappen opnieuw te doorlopen. • Kijk naar de experts die noodzakelijk zijn voor de validatie van algoritmen. Op welke wijze hebben zij dit in eerdere trajecten uitgevoerd en welke methodieken zijn hierbij gehanteerd? Welke lessen kunnen hieruit getrokken worden voor jouw traject? Er is altijd een veelvoud aan validatie technologie aanwezig maar probeer aan te sluiten bij peers uit het veld die soortgelijke analyses hebben toegepast in data trajecten. • Interpreteer de modellen op basis van domeinkennis, succescriteria en het gewenste testontwerp en check met bedrijfsanalisten en domeinexperts om de resultaten te bespreken. Houd ook rekening met alle andere resultaten die in de loop van het project zijn geproduceerd. • Kijk ook naar Europese standaarden voor statistiek, welke statistische principes worden gehanteerd. • Pas de principes van responsible Data Science – zoals FACT (Fairness – Accountability – Confidentiality – Transparency) toe. • Wat kun je in en proeftuinvoorziening verder uittesten, door ontwikkelen of weer een stap terug doen. • Onderzoek ook welke trainingsinstanties eventueel verantwoordelijk waren voor fouten (o.a. bij het toepassen van RNN's). • Een optie is om falsificatie te gebruiken, bijvoorbeeld als correlaties verschillen, is dan	Controle over technologie/ algoritmes, vertrouwen, veiligheid van het systeem, transparantie, gelijkheid, inclusiviteit, voorkomen willekeur, voorkomen discriminatie
---------------------------------	---	---	--

	○ Wat doet het met de data (parametrisering) ○ Wat komt er uit (selectie, patroon)? ○ Wat is de kwaliteit of de fit van het model? • In hoeverre wordt door het model geproduceerde data 'vastgehouden' i.v.m. de reproduceerbaarheid van de uitkomsten van een model? • Op welke wijze voegen deze methodieken daadwerkelijke informatie waarde toe aan de analyse kijkend naar de aard van de dataset? Beschrijf de feedbackloop in het modelleringsproces > heeft het modelleren geleid tot aanpassingen in de datapreparatie? • Is het model getoetst door andere partijen, zo ja door wie en op welke wijze?	duidelijk wie wat vindt? Dit kan gezien worden als een interne challenge, een soort PEN-test. • Probeer ook de frictie op te zoeken en het niet alleen met elkaar eens te zijn ten aanzien van het komen tot uitkomsten van een model. • Welke specifieke infrastructuurvoorziening moet hiervoor 'in place' zijn.	
Fase 4 – (afsluitende vraag fase 4)	• Zijn er nog andere onderwerpen die men ter sprake wenst te laten komen? • Heeft men iets geleerd waardoor aanpassing in de bedrijfsdoelstelling noodzakelijk is?	• Indien wordt gesignaleerd dat aanpassing in eerdere fase noodzakelijk is dienen alle vragen wederom doorlopen te worden.	Controleerbaarheid van het systeem, transparantie, validiteit
Fase 5 – Evaluatie	• Draagt de modellering bij aan het beoogde business doel? Zijn er onverwachte uitkomsten? Toetsen aan KPI's? KSF's? • Welke resultaten laten eerste tests zien? Doet het wat het doen moet of levert het vreemde dingen op? Zijn er dingen die je niet verwacht had? • Zijn er nieuwe juridische/ethische/maatschappelijke risico's zichtbaar geworden die vooraf niet ingeschat zijn? • Check het gehele ontwikkeltraject > zijn er stappen over het hoofd gezien?	• Indien er fouten zichtbaar zijn >> niet deployen. De implementatie moet geen doel op zich worden. Ook een niet succesvol traject is een resultaat. • R&D is ook falen in ontwikkeling aangezien ook hier wetenschap uit wordt verkregen. • Gaat het nu om het toepassingsresultaat of mag het een leerstap naar het volgende zijn? Er moet worden nagedacht over vooruitstappen na de pilot. Ook leren van je fouten en willen doorstappen naar andere toepassing.	Controleerbaarheid van het systeem, transparantie, validiteit, voorkomen detournement de pouvoir, machtsverhoudingen (rechtszekerheid in taakuitvoering), privacy

		• Als er bepaalde veranderingen noodzakelijk zijn niet in de infrastructuur zelf aanpassen maar in de proeftuin voorziening zodat je kennis hebt in de pilot en vervolgstappen. • Leer slim van je fouten en denk van te voren na over tussenliggende infrastructuur die je nodig hebt.	
Fase 6 – Deploy	• Uitrol, is dit voldoende? Welke verbeteringen zijn nog mogelijk. • Het model tijdens het gebruik constant blijven evalueren. • Hoe is beheer op het model geborgd? • Klopt het model of zijn er ergens fouten gemaakt? • Klopt de datapreparatie? Kloppen de aannames over de data (bijvoorbeeld verdeling) en passen deze bij het model? • Is er een continue feedbackloop ingebouwd na de deploy? • Hoe worden de resultaten gevalideerd? • Hoe worden de resultaten gebruikt in de Operatie, is er sprake van autonoom gebruik of 'human in the loop'.	• Let op, bij zelflerende algoritmen moeten we nog steeds goed signaleren in hoeverre er verschillen in uitkomsten optreden op basis van o.a. feedback loops er hertrainen. Dit kan ook resulteren in een ongewenste bias. • De laatste vraag is om te kunnen bepalen of er sprake is van automatische besluitvorming (pre-GEB).	Voorkomen detournement de pouvoir, machtsverhoudingen (rechtszekerheid in taakuitvoering), privacy, controle op technologie en algoritme, transparantie, veiligheid van de maatschappij, bescherming mensenrechten, databescherming, voorkomen van willekeur

Titel:	
Doelbinding: <i>Wat is de doelbinding van dit profiel?</i>	
Bronnen: <i>Welke bronnen zijn gebruikt om tot dit profiel te komen? Als het gaat om een document of rapportage, noem dan het exacte document.</i>	Kwaliteit van de bronnen: <i>Wat is de kwaliteit van deze bronnen? Hoe objectief of subjectief zijn ze?</i>
Analyse: <i>Noteer hier de analyse en beschrijf hoe en waarom je tot bepaalde conclusies komt. Probeer zo compleet mogelijk te zijn. Als iemand anders dan jij het leest, moeten zij kunnen begrijpen hoe en waarom jij tot je conclusies bent gekomen.</i>	
Het profiel: <u>Indicator in PNR</u>	<u>Waarde</u>

Profielen



Titel: Profiel kindersmokkel	
Doelbinding: Het onderkennen van hulp aan minderjarigen bij illegale toegang, zoals strafbaar gesteld in artikel 197a SR, per vliegtuig tot Nederland.	
Bronnen: <i>Welke bronnen zijn gebruikt om tot dit profiel te komen? Als het gaat om een document of rapportage, noem dan het exacte document.</i>	Kwaliteit van de bronnen: <i>Wat is de kwaliteit van deze bronnen? Hoe objectief of subjectief zijn ze?</i>
- Bedrijfsprocessensysteem (BPS); - Vreemdelingen Basis Systeem (VBS); - Basisvoorziening Vreemdelingen (BVV); - Opsporingsapplicatie Summ-I.T.;	In principe objectieve bronnen, registratie van feiten. Wel afhankelijk van wijze registreren collega, betreft tevens subjectieve verklaringen van gehoorde personen.
- Verkenning PNR gegevens via Passagiersinformatie-eenheid Nederland;	Objectieve bron, registratie van passagiersgegevens. Wel afhankelijk van aangeleverde informatie door luchtvaartmaatschappijen.
- Informatie-uitwisseling pre-boarding adviseurs KMar, Art. 10 (2) (d) [redacted];	Objectieve bron, registratie van adviezen, wel afhankelijk van beschikbare tijd, pre-boardinginformatie daarnaast formeel nog niet deelbaar.
- Europol, Art. 10 (2) (c) [redacted]; - Europol, [redacted]; - Europol, [redacted];	Objectieve bron, doel is elkaar als lidstaten te informeren, wel afhankelijk van juiste invoer van lidstaten.
- Frontex, Art. 10 (2) (c) [redacted]; - Frontex, [redacted]; - Frontex, [redacted]; - Frontex, [redacted]; - Frontex, [redacted];	Objectieve bron, informatie o.a. gebaseerd op risico-analyse van intelligence, wel afhankelijk van invoer lidstaten.

Analyse:

Noteer hier de analyse en beschrijf hoe en waarom je tot bepaalde conclusies komt. Probeer zo compleet mogelijk te zijn. Als iemand anders dan jij het leest, moeten zij kunnen begrijpen hoe en waarom jij tot je conclusies bent gekomen.

In [redacted] werd reeds een [redacted] veroordeeld voor het smokkelen van [redacted] kinderen binnen de periode Art. 10 (2) (c) vanuit [redacted] naar Nederland. De rechtbank gaf aan dat door mensensmokkel niet alleen het overheidsbeleid inzake bestrijding van illegaal verblijf in en illegale toegang tot Nederland en andere landen van de Europese Unie wordt doorkruist, maar ook wordt bijgedragen aan het in standhouden van een illegaal circuit, waardoor het maatschappelijk verkeer wordt of kan worden gefrustreerd en gecorrumpeerd, terwijl het beeld en de positie van de 'echte' asielzoeker daardoor kan worden geschaad. [redacted]

[redacted] In [redacted] werden op zowel [redacted] als [redacted] gedurende [redacted] opnieuw verschillende mensensmokkelzaken geregistreerd waarbij minderjarigen vanuit [redacted] naar Nederland gesmokkeld werden. Tevens adviseerde de Marechaussee in [redacted] collega's bij het pre-boarden in een heel aantal zaken waarbij gepoogd werd minderjarigen irregulier mee te nemen op een vlucht naar zowel [redacted] als [redacted]. Uit de zaken in [redacted] kwamen onder meer de volgende kenmerken naar voren:

- Art. 10 (2) (c) [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Daarnaast blijkt dat:

- Art. 10 (2) (c) [redacted]
- [redacted]

Dat de problematiek Europa breed speelt blijkt onder meer uit rapportages van Europol en Frontex. In de smokkelzaken van minderjarigen benoemd in deze rapportages komt [redacted] veelvuldig naar voren, o.a. op routes naar Art. 10 (2) (c) [redacted] werden zaken geregistreerd. Waar op routes naar Nederland enkele zaken speelden met [redacted], werden ook binnen Europa naast de zaken van [redacted] verschillende andere [redacted] benoemd waaronder de betrokkenheid van [redacted]. Daarbij werd vaker gerapporteerd over zaken waarin [redacted] en waarbij in verschillende zaken [redacted]

¹ Art. 10 (2) (c) [redacted]

Het profiel: <u>Indicator in PNR</u>	<u>Waarde</u>
 Art. 10 (2) (C)	 Art. 10 (2) (C)
	
	
	
	
	