BIJLAGE Implementatieplan waarborgenkader

1. Aanleiding en doel

Voor u ligt een nota waarin een basisuitwerking staat beschreven van een kwaliteitssysteem en daarbij horend waarborgenkader algoritmegebruik wat op de context van de Douane is toegesneden. Er is hierbij voortgeborduurd op het reeds binnen de Douane bestaande kwaliteitssysteem (ondersteund door DOU-IT[1]) wat gaandeweg de jaren is ontwikkeld, en toonaangevende Europese- en Rijkskaders op dit gebied.

Hoewel er in deze nota ingezoomd wordt op algoritmen is de opzet van genoemd kwaliteitssysteem breder toepasbaar.

Dit document beschrijft achtereenvolgens:
- De context voor het kwaliteitssysteem, door een beschrijving te geven van de algoritmen die binnen de Douane gebruikt worden (hoofdstuk 2)
- Een overzicht van de wettelijke kaders die eisen stellen aan het ontwerp van het kwaliteitssysteem voor algoritmen of deze anderzijds beïnvloeden, en de Douane invulling van deze wettelijke kaders (hoofdstuk 3)
- Een beschrijving van het ontwerp van het kwaliteitssysteem voor algoritmen (hoofdstuk 4)
- Een overzicht van de lopende beproevingen rondom kwaliteitswaarborgen binnen de Douane (hoofdstuk 5)
- Een aanpak om tot een verdere professionalisering van het kwaliteitssysteem te komen.

Maatschappelijk en politiek ligt de inzet van AI en algoritmen onder een vergrootglas. Bij eerdere inzet door andere overheidsdiensten zijn problemen gerezen rond ongeoorloofd gebruik van data en onnauwkeurigheid of onvoorspelbaarheid van de werking en uitkomsten. Dit heeft geleid tot problemen bij o.a. Toeslagen (één van de aspecten van het rapport Ongekend Onrecht) en in de sociale sector (het Systeem voor Risico Indicatie - SYRI).

Als Douane willen we waarborgen scheppen om de kwaliteit van algoritmen te verhogen en de mogelijke risico's tijdens de inzet ervan te mitigeren. In deze nota worden de stappen uiteengezet die nodig zijn om te komen tot een kwaliteitssysteem voor het deugdelijk ontwikkelen en beheren van zowel in gebruik zijnde (eenvoudige risico-regel) algoritmen als in ontwikkeling zijnde (geavanceerde AI) algoritmen.

Met hulp van dit - op de douanecontext toegesneden - kwaliteitssysteem heeft de Douanecontrole op de inzet van algoritmen en kan zij dit ook richting belanghebbenden, zoals toezichthouders, burgers en de maatschappij, als geheel verantwoorden. Hiermee zorgt zij dat de kansen die algoritmen (bijvoorbeeld gebruikmakend van AI-technologie)[2] haar biedt ten volste benut kunnen blijven worden.

De douaneorganisatie heeft kwaliteit hoog in het vaandel staan. Borgen dat we de goede dingen juist doen zodat we onze handhavingsstrategie optimaal kunnen uitvoeren. Hierin hebben we de afgelopen jaren reeds grote stappen gezet, bijvoorbeeld door middel van de realisatie en procesmatige inrichting rond DOU-IT en de professionalisering van de datascience functie. Maar we zien ook dat er op enkele punten nog kwaliteitsverbeteringen mogelijk zijn. Met hulp van dit kwaliteitssysteem heeft de Douane de mogelijkheid deze te realiseren.

2. Context, het gebruik van algoritmen binnen de Douane

De Douane gebruikt, net zoals de rest van de Rijksoverheid, al tientallen jaren eenvoudige algoritmen ter ondersteuning van haar werkzaamheden. Dit betreft de zogenaamde risico-regels. Door ontwikkelingen als volumegroei (o.a. e-commerce) en de versterkte aanpak op ondermijning, heeft de Douane daarnaast voor de doorontwikkeling van haar takenpakket nieuwe (innovatieve) vormen van geavanceerde algoritmen nodig.

Inzetgebied Douane

[1] DOU-IT is een applicatie waarin terug is te vinden hoe het algoritme (prismaprofiel) tot stand is gekomen.
[2] Onder AI-technologie worden machines verstaan die dingen doen die intelligentie vereisen wanneer mensen dezelfde dingen zouden doen.

Douane werkt risicogericht. Ze kent verschillende opdrachtgevers, die per handhavingsgebied aangeven waarop gehandhaafd moet worden. Uit deze opdrachten vloeien handhavingsactiviteiten voort waarbij algoritmen gebruikt worden om patronen te ontdekken in de data (over de logistieke goederenstroom), die duiden op een verhoogde kans dat er een risico aanwezig is. Dat kan zowel een fiscaal-, accijns- en VGEM-risico zijn. Tijdens training 'leert' het algoritme deze patronen te herkennen en bij de toepassing kan de aanwezigheid van een dergelijk patroon of afwijking op een normaalpatroon leiden tot een mogelijke nadere inspectie van de goederen.

Het gebruik en doorontwikkeling van algoritmen binnen de Douane wordt als wenselijk en noodzakelijk gezien. Zo leidt e-commerce tot sterk stijgende aangiftevolumes (datavolumes) en noopt de aanpak van complexe problematiek zoals ondermijning ertoe om data optimaal te gebruiken. De inzet van algoritmen helpen ons hierbij. Daarnaast is de verwachting dat de "hit-rate" significant verbeterd wordt bij inzet van geavanceerde algoritmen. De inzet van geavanceerde algoritmen biedt dus zowel de mogelijkheden om de groeiende datavolumes aan te kunnen als een effectievere handhaving.

Definitie algoritme, eenvoudige en geavanceerde algoritmen
Algemene definities van wat een algoritme is zijn erg breed. De uitdaging is daarom om een definitie te geven die de Douane-praktijk weerspiegelt en handvatten biedt voor een uitlegbare controle-strategie. Als Douane hebben we de volgende overwegingen in ogenschouw genomen rondom de definitie van een algoritme en de typen algoritmen.

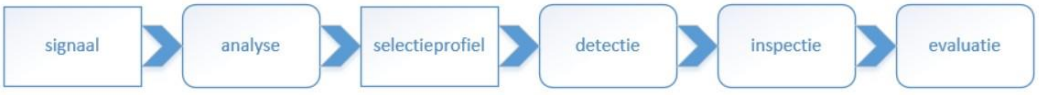
De definitie van een algoritme van de Algemene Rekenkamer (ARK), die bijvoorbeeld ook door Binnenlandse Zaken is overgenomen als conceptdefinitie ten behoeve van het algoritmeregister, is breder dan de definitie van AI-systemen uit de AI Act van de EU. De AI act beperkt zich tot systemen met een mate van kunstmatige intelligentie, terwijl de ARK-definitie in de basis elke vorm van programmatuur omvat.

"Een set van regels en instructies die een computer geautomatiseerd volgt bij het maken van berekeningen om een probleem op te lossen of een vraag te beantwoorden. Algoritmes kennen zeer uiteenlopende verschijningsvormen van rekenmodellen, beslisbomen en andere statistische analyses tot complexe dataverwerkingsmodellen en 'zelflerende' toepassingen."[3]

Omdat het niet de bedoeling is om alle software te omvatten, is er een afbakening nodig. De Douane maakt op hoofdlijnen onderscheid tussen eenvoudige en geavanceerde algoritmen, waarbij in de laatste categorie gebruik gemaakt kan worden van AI-technologie. In onderstaande paragrafen staat nader toegelicht wat onder eenvoudige en geavanceerde algoritmen wordt verstaan.

Het gaat de Douane hierbij om de risico's die voortkomen uit het gebruik van het algoritme en of er voldoende mitigerende maatregelen zijn genomen ter afdekking van die risico's, of dat mogelijke restrisico's bestuurlijk zijn afgedekt. Het maakt hierbij niet uit of het een eenvoudig algoritme of geavanceerd algoritme betreft. Hiermee volgt de Douane de lijn die ook op landelijk niveau wordt aangehouden.

Eenvoudige algoritmen
Binnen de Douane zijn op dit moment enkel eenvoudige algoritmen, ook wel risico-regels, selectie-instrument of prismaprofiel[4] genoemd, in gebruik. De werkwijze hiervan binnen de Douane processen ziet er sterk vereenvoudigd als volgt uit:



Naar aanleiding van een verkregen signaal kan er een analyse worden gestart om te bepalen of het wenselijk is dit op te nemen in een selectieprofiel, bijvoorbeeld omdat het een daadwerkelijk geconstateerd risico (relevant risico) betreft, of een risico dat naar verwachting kan/zal voorkomen (theoretisch of potentieel risico). Bij de inzet van het selectieprofiel kan dit

[3] Bron: Aandacht voor Algoritmes; Algemene Rekenkamer (2021).
[4] PRISMA is een applicatie waarmee de risico detectie wordt uitgevoerd

op basis van de hierin opgenomen criteria tot een detectie leiden waarna vervolgens door een specialist wordt bepaald welke gevallen daadwerkelijk geïnspecteerd dienen te worden[5]. Aan de hand van de uitkomsten van de gedane inspecties vindt er periodiek een evaluatie plaats wat mogelijk tot bijstelling van het selectieprofiel leidt.

Deze stappen worden allemaal administratief vastgelegd in DOU-IT waardoor altijd terug is te vinden hoe het algoritme (prismaprofiel) tot stand is gekomen en welke wijzigingen mogelijk hebben plaatsgevonden.

Geavanceerde algoritmen
In het Strategisch Meerjarenplan Douane en het Jaarplan 2022 is benoemd dat de Douane met behulp van data en algoritmen beter grip wil krijgen op risicovolle goederen en niet-compliant aangiftegedrag. Een vorm van geautomatiseerde risicodetectie is noodzakelijk om toezicht te houden op de sterk groeiende goederenstroom. Bovendien moet de uitworp van de risicoselecties uitvoerbaar en accuraat zijn, dat wil zeggen, die moet de controle-capaciteit niet overschrijden en door een goede hitrate tot minder onterechte controles leiden.

Om deze doelen te bereiken zijn geavanceerde algoritmen nodig[6], waarvan de ontwikkeling bij de Douane als "autodetectie" is ondergebracht in het Strategisch Meerjarenplan. Ook bij deze geavanceerde algoritmen stelt de Douane bij de keuze voor een te gebruiken techniek de eis dat deze transparant en uitlegbaar moet zijn. Best-practices uit de algoritme-ontwikkeling kunnen het ontwikkelproces documenteren en transparant houden. Welke uitleg en mate van transparantie gewenst en noodzakelijk zijn, is organisatie-specifiek en kan voor verschillende processen bij de Douane vastgesteld worden. Bij de Douane is een verkenning gedaan door een promotiestudent met zijn onderzoek naar de benodigde uitlegbaarheid voor verschillende doelgroepen medewerkers. De voorgestelde Europese AI Act (zie paragraaf wettelijke kaders) biedt handvatten voor het inschatten van het risico bij het gebruik van algoritmen.

Er zijn dus algoritmen in vele varianten, variërend van eenvoudig tot geavanceerd. In alle varianten is het is belangrijk dat duidelijk is hoe het algoritme tot haar resultaat is gekomen, hoe het is opgebouwd en welke gegevenselementen daarbij een rol hebben gespeeld. Als Douane hechten we namelijk groot belang bij het ten alle tijden weten waarom een zending als risicovol wordt aangemerkt.

Risicovolle algoritmen
Vooruitlopend op de beschrijving van de wettelijke kaders die van toepassing zijn op het kwaliteitssysteem voor algoritmen van de Douane, is het belangrijk om de categorisering van risicovolle algoritmen te beschrijven. In de Europese Unie wordt momenteel gewerkt aan de AI Act. Hierin worden regels opgesteld voor diverse AI-systemen. De Europese Commissie heeft daarbij gesteld dat de verordening niet mag leiden tot belemmering van de ontwikkeling van veilige AI. De tekst is nog niet definitief omdat de Raad nog moet instemmen en daarna pas het Europees Parlement zich erover buigt. De AI Act specificeert onder meer hoog risico AI-systemen, waaraan onder andere een registratieverplichting verbonden is en eisen gesteld worden aan het kwaliteitssysteem. De AI Act is derhalve ook relevant voor het ontwerp van het kwaliteitssysteem voor algoritmen van de Douane.

AI-systemen worden in de AI act als hoog risico gezien, tenzij het AI-systeem louter ondergeschikt is met betrekking tot de relevante actie of te nemen beslissing en daarom waarschijnlijk niet zal leiden tot een significant risico voor de gezondheid, veiligheid of fundamentele rechten. De kenmerken van het ondergeschikt zijn, werkt de Europese Commissie nog nader uitwerken. De AI Act geeft de Europese Commissie de ruimte om in de toekomst AI-systemen toe te voegen. Hierbij zal de Commissie kijken naar de volgende criteria:
- het beoogde doel van het AI-systeem;
- de mate waarin een AI-systeem is gebruikt of waarschijnlijk zal worden gebruikt;
- de mate waarin het gebruik van een AI-systeem al schade heeft toegebracht aan de gezondheid en veiligheid of negatieve gevolgen heeft voor de grondrechten of aanleiding heeft gegeven tot aanzienlijke bezorgdheid met betrekking tot de verwezenlijking van dergelijke schade of negatieve gevolgen, zoals blijkt uit rapporten of gedocumenteerde beschuldigingen ingediend bij nationale bevoegde autoriteiten;

[5] Met uitzondering van de fiscale selecties. Deze worden semi-geautomatiseerd aan het primair proces aangeboden.
[6] Patronen worden middels AI-technieken afgeleid uit data in tegenstelling tot bij eenvoudige algoritmen waar signaal wordt ingebracht door mens.

- de potentiële omvang van dergelijke schade of dergelijke nadelige gevolgen, met name wat betreft de intensiteit en het vermogen om meerdere personen te treffen;
- de mate waarin potentieel benadeelde of benadeelde personen afhankelijk zijn van het resultaat dat met een AI-systeem wordt bereikt, met name omdat het om praktische of juridische redenen redelijkerwijs niet mogelijk is om van dat resultaat af te zien;
- mate waarin potentieel benadeelde of benadeelde personen zich in een kwetsbare positie bevinden ten opzichte van de gebruiker van een AI-systeem, met name door een onbalans in macht, kennis, economische of sociale omstandigheden of leeftijd;
- de mate waarin de met een AI-systeem geproduceerde uitkomst niet gemakkelijk omkeerbaar is, waarbij uitkomsten die van invloed zijn op de gezondheid of veiligheid van personen niet als gemakkelijk omkeerbaar worden beschouwd;

Binnen de Rijksoverheid vormt de Europese AI act een uitgangspunt, maar worden op nationaal niveau aanvullende eisen gesteld[7]:
- In de eerste plaats worden definitie en reikwijdte verbreed zodat ook de eenvoudige algoritmen met hoog risico hier onder vallen.
- In de tweede plaats gaat het om overheidsalgoritmen die, zoals in de werkagenda staat aangegeven, gecontroleerd worden op discriminatie, transparantie en willekeur.

Binnen de reikwijdte van het kwaliteitssysteem voor de Douane wordt hiermee een algoritme (zowel een eenvoudig algoritme als een geavanceerd algoritme) als hoog risico gezien indien deze aan de volgende criteria voldoet:
- Het algoritme is in gebruik door een bestuursorgaan of een onder diens verantwoordelijkheid werkzame instelling, dienst of bedrijf.
- Het algoritme wordt gebruikt in, of ter ondersteuning van een taak of proces waar voor de overheid bijzondere normen gelden om burgers, bedrijven en samenleving te beschermen tegen de overheid.
- De taak of het proces waarin/waarbij het algoritme wordt gebruikt, heeft meer dan slechts een ondergeschikte inhoudelijke invloed op de positie van de burger/samenleving. (Met andere woorden: impact van taak/proces op de burger/samenleving is groot)
- Het algoritme (en de toepassing daarvan) heeft meer dan slechts ondergeschikte invloed op de taak of het proces. (Met andere woorden: impact van het algoritme op de taak/het proces is groot)

Het is hierbij voor de Douane van belang dat zij het evenwicht zoekt tussen wat we (vanuit wet- en regelgeving) moeten doen en de facilitering van het bedrijfsleven. Het moet in balans zijn. Het wordt niet anders dan wat we nu ook doen (immers een van onze douanedoelstelling luidt: Bescherming van de samenleving!). Géén of minder douanecontroles heeft daarom een veel grotere impact op de samenleving.

3. Wettelijke kaders

Het werkveld van waarborgen rond het gebruik van algoritmen kent vele invalshoeken. Er is dan ook reeds een heel palet aan kaders voor ontwikkeld en dit zal, mede gezien de maatschappelijke aandacht, de komende tijd alleen maar toenemen is de verwachting.

De Douane krijgt, opeenvolgend in belangrijkheid, te maken met Europese kaders en Rijksbrede kaders[8]. Daarnaast zijn er meerdere buiten het ministerie gelegen toetsingsautoriteiten zoals de Audit Dienst Rijk (ADR) en Autoriteit Persoonsgegevens (AP) waar we als Douane mee te maken hebben, en krijgen, gegeven de recent opgerichte algoritme waakhond.

Dit alles resulteert in een inperking van de bestuurlijke keuzeruimte van de Douane wat haar noodzaakt meer aan de voorkant van het proces mogelijke kaderstelling te beïnvloeden.

De belangrijkste kaders voor de Douane op dit moment zijn:
- Europese AI Act
- Rijksbreed implementatiekader voor inzet algoritmen

[7] Werkdocument algoritme met impact 25 november 2022
[8] Europese wetten gelden boven nationale wetten. Er zijn twee vormen van Europese regels: een Europese verordening is na inwerkingtreding meteen ook een Nederlandse wet. Europese richtlijnen moeten binnen een bepaalde termijn worden omgezet in nationale wet- en regelgeving, meestal binnen twee jaar nadat het besluit genomen is. Bron: www.tweedekamer.nl

Deze worden hieronder kort beschreven.

Europese AI Act
De Europese Commissie heeft een nieuwe verordening voor AI voorgesteld, omdat zij meent dat de huidige Europese regelgeving de (toekomstige) risico's van AI onvoldoende adresseert. Deze verordening heeft een op risico gebaseerde aanpak: hoe meer risico de technologie met zich meebrengt, hoe strikter de regels die ervoor gelden.

Rijksbreed implementatiekader inzet van algoritmen
Bestaande juridische kaders bieden waarborgen voor een verantwoorde inzet van algoritmische risicomodellen en andere verwerkingen. Deze waarborgen zijn vaak in algemene termen omschreven. Dat vraagt in de praktijk om een vertaalslag naar concrete instrumenten en hulpmiddelen, zoals het Impact Assessment Mensenrechten en Algoritmen (IAMA)[9], de handleiding "Privacy by design"[10], de handreiking "Non-discriminatie by design"[11], de Code Goed Digitaal Openbaar Bestuur (CODIO)[12], het Toetsingskader algoritmen van de Algemene Rekenkamer[13] en het mensenrechtelijk toetsingskader 'Discriminatie door risicoprofielen' van het College voor de Rechten van de Mens[14].
Deze en andere hulpmiddelen en instrumenten worden samengevoegd en beter met elkaar in samenhang gebracht in het *implementatiekader inzet van algoritmen*. Belangrijke onderdelen hiervan zullen een verplichtend karakter kennen. Dit schept duidelijkheid aan overheidsinstellingen over de eisen waar ze aan moeten voldoen, wat van ze wordt verwacht en zorgt dat er duidelijkheid bestaat in welke gevallen, welk instrument of hulpmiddel wordt ingezet bij de inzet van algoritmen in de werkprocessen.[15]

Algoritmeregister
Een onderdeel uit het implementatiekader inzet van algoritmen dat op dit moment wordt ontwikkeld, is het algoritmeregister. Het algoritmeregister richt zich op het algemeen publiek, in het bijzonder burgers en bedrijven die te maken hebben met de Douane.

Het kabinet wil hiermee de transparantie bij de ontwikkeling van alle hoog-risico algoritmen (publiek en privaat) vergroten. Het kabinet vindt het belangrijk dat burgers de overheid kunnen volgen en kritisch kunnen bevragen of zij zich aan de regels houdt. Daarom gaat het kabinet voor overheidsorganisaties het opstellen van een algoritmeregister verplicht stellen. Uitgangspunt is dat overheden zelf verantwoordelijk zijn voor het opstellen en beheren van een algoritmeregister. Het algoritmeregister bevat in ieder geval hoog-risico algoritmen. Het kabinet werkt aan het op een centrale plek toegankelijk maken van algoritmen, gevoed door informatie over algoritmen die overheidsorganisaties publiceren op hun eigen internetpagina.[16]

Op basis van de in hoofdstuk 2 genoemde criteria komen algoritmen die direct of indirect rechtsgevolgen hebben voor burgers of bedrijven of deze anderszins in aanzienlijke mate treffen in aanmerking voor publicatie in het algoritmeregister. Hierbij valt te denken aan de kofferselectie op de luchthaven of e-commerce pakketjesselectie.

Indien openbaarmaking leidt tot concrete en reële risico's voor de uitvoering van de taken van de Douane, kiest de verantwoordelijke directeur ervoor een deel van de informatie over een algoritme niet openbaar te maken. Bijvoorbeeld wanneer het delen van grenswaarden uit een selectie-indicator er vermoedelijk toe leidt dat burgers en bedrijven op een oneigenlijke wijze anticiperen op een selectie.

Voordat de verantwoordelijk directeur hiervoor kiest, maakt hij of zij een belangenafweging tussen het belang van de Douane, het belang van de burger en het belang van transparant zijn. De belangenafweging wordt onderbouwd vastgelegd en zal door de Chief Data Officer (CDO) met een advies aan het MT ter besluitvorming worden aangeboden[17]. De DG Douane is voorzitter van het MT en neemt daarmee het besluit.

---

[9] https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes
[10] https://www.cip-overheid.nl/productcategorieën-en-workshops/producten/privacy-bescherming/#handleiding-privacy-by-design
[11] https://www.rijksoverheid.nl/documenten/rapporten/2021/06/10/handreiking-non-discriminatie-by-design
[12] https://www.tweedekamer.nl/kamerstukken/detail?id=2021D22774&did=2021D22774
[13] https://www.rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader
[14] https://www.rijksoverheid.nl/documenten/rapporten/2021/11/30/discriminatie-door-risicoprofielen--mensenrechtelijk-toetsingskader
[15] Motie van Kamerleden Bouchallikh (GroenLinks) en Dekker-Abdulaziz (D66) c.s. (Kamerstukken II 2021/22, 26643, nr. 835)
[16] https://standaard.algoritmeregister.org
[17] Concrete uitwerking van dit proces zal later in separaat beleidskader worden vastgelegd

Invulling van deze kaders voor de Douane
Binnen de Douane willen we een kwaliteitssysteem dat op de Douane context is toegesneden, waarbij een algoritme de toetsing en waarborgen krijgt die de aard van het proces vereist[18].

Wanneer we een algoritme dat wordt toegepast binnen de Douane werkprocessen kunnen classificeren binnen een categorie van de Europese AI Act, kunnen we uit het ADR-normenkader de relevante regels voor het gebruik van dit algoritme van toepassing verklaren. Deze werkwijze is nodig omdat het ADR-normenkader op dit moment uitgaat van een set normen die op alle typen algoritmen van toepassing is. Het is dus ontworpen op de zwaarste categorie algoritmen, en veel regels richten zich op aspecten van privacy, discriminatie, onrechtmatige beïnvloeding etc.

Hoewel het ADR-normenkader hiermee haar kracht bewijst is, is het ook belangrijk om onderscheid te maken tussen de categorieën algoritmen (zoals eenvoudig en geavanceerd), en wat de toepassing en datagebruik is van het algoritme. Wanneer bijvoorbeeld een containerscan door een algoritme wordt beoordeeld op de aanwezigheid van drugs, spelen aspecten van privacy of discriminatie van natuurlijke personen geen rol. Daarnaast worden (voor zover nu voorzien) algoritmen binnen de Douane slechts gebruikt als signalering die leidt tot nadere inspectie door mensen – er worden geen volautomatische beslissingen genomen, al zou dit mogelijk in de toekomst kunnen wijzigen.

In de context van de Douane geldt dat hetzelfde normenkader op dezelfde wijze toepassen op *alle* algoritmen leidt tot een zeer zwaar middel dat haar doel voorbijstreeft. De Douane geeft de voorkeur aan meer maatwerk: we willen de inzet van algoritmen (zoals selectie-instrumenten) de toetsing en de waarborgen geven die de aard van het proces vereist. Hiermee volgt de Douane de algemene tendens binnen de Rijksoverheid rond het creëren van waarborgen bij de inzet van algoritmen in brede zin, in lijn met de aankomende Europese AI-verordening.

De invulling en toepassing van het kwaliteitssysteem op een individueel algoritme is dus afhankelijk van het type algoritme, maar bovenal van het risico dat (het gebruik van) een algoritme met zich meebrengt. Deze risico-gebaseerde toepassing van het kwaliteitssysteem per algoritme volgt dus een gestandaardiseerde risicodeling (zie ook hoofdstuk 4). Deze risicodeling is onder andere afhankelijk van het type algoritme (e.g. eenvoudig of geavanceerd algoritme), de gebruikte data (e.g. of persoonsdata wordt gebruikt of niet), mate van automatisering (e.g. vindt geautomatiseerde besluitvorming plaats of niet) en het toepassingsgebied van het algoritme (e.g. de mate waarin de kernprocessen van de Douane geraakt worden als het algoritme niet functioneert).

4. Ontwerp kwaliteitssysteem

Voor waarborgen die passen bij de typen algoritmen en context van de Douane (zie hoofdstuk 2) en voldoen aan wettelijke kaders (zie hoofdstuk 3), is een passend kwaliteitssysteem nodig. Dit kwaliteitssysteem bevat alle onderdelen die nodig zijn om deze waarborgen in de praktijk in te richten en uit te voeren.

Binnen de Douane willen we een op de douanecontext toegesneden kwaliteitssysteem gebruiken om de kwaliteit van algoritmen te verhogen en de mogelijke risico's tijdens de inzet ervan te mitigeren. Hierdoor zijn we als Douane in control bij de inzet van algoritmen en kunnen we ons richting de maatschappij verantwoorden.

Daarnaast heeft de douaneorganisatie kwaliteit hoog in het vaandel staan. Borgen dat we de goede dingen juist doen zodat we onze handhavingsstrategie nog beter kunnen uitvoeren. Hierin hebben we de afgelopen jaren reeds grote stappen gezet bijvoorbeeld middels de realisatie en procesmatige inrichting rond DOU-IT en de professionalisering van de datascience functie. Maar we erkennen ook dat er op enkele punten nog kwaliteitsverbeteringen mogelijk zijn. Middels dit - op de douanecontext toegesneden – kwaliteitssysteem heeft de Douane de mogelijkheid deze te realiseren.

[18] MT Douane 22 Maart 2022 Gebruik algoritmen Douane

Bestuurlijke keuzeruimte
Als zelfstandige Directeur-Generaal (DG) heeft de Douane een bepaalde mate van bestuurlijke keuzeruimte hoe zij invulling geeft aan haar verantwoordelijkheid rond het verantwoord gebruik van algoritmen binnen de Douane alsook welke kwaliteitsverbeteringen zij wil bewerkstelligen.

Er zou voor geopteerd kunnen worden om met name in te zetten op het inregelen van voldoende waarborgen voor enkel geavanceerde hoog risico algoritmen, omdat de Europese AI Act dit op korte termijn gaat verplichten. Hiermee negeer je echter de kwaliteitsverbeteringen rond het gebruik van eenvoudige algoritmen (feitelijk de kern van de Douane handhavingsstrategie op dit moment) die de Douane kan bewerkstelligen. Daarnaast volgen we dan niet de lijn (brede definitie van een algoritme) die momenteel op overheidsbreed zichtbaar is.

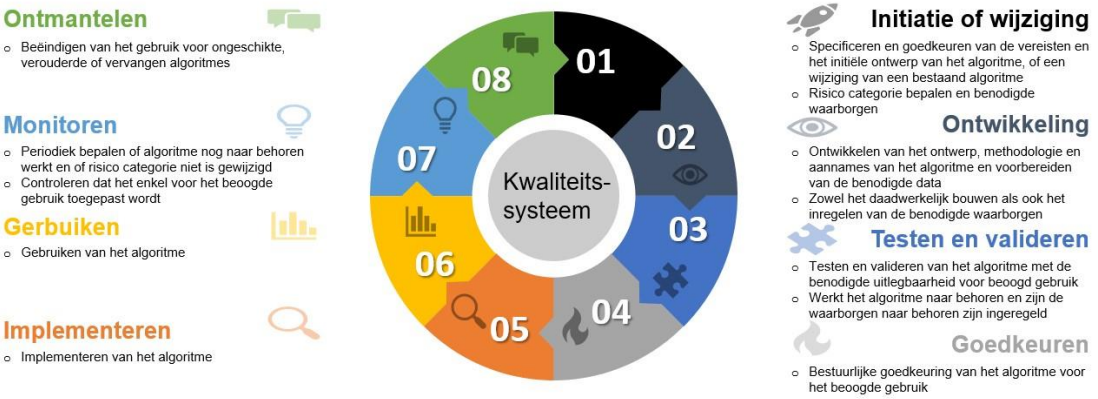
Middels deze nota willen we dan ook adviseren om er als Douane voor te kiezen om gelijk voldoende waarborgen voor zowel eenvoudige- als geavanceerde algoritme in te regelen. Hiermee bewerkstelligt de Douane niet alleen de benodigde kwaliteitsverbeteringen in de actuele inzet van algoritmen (geavanceerde algoritmen worden nog niet ingezet) binnen de Douane. Maar we sorteren hiermee ook voor op de lijn die momenteel op landelijk niveau zichtbaar is. Door hier nu al mee aan de slag te gaan, naast het meer aan de voorkant beïnvloeden van het proces rond aankomende kaderstelling (zoals het Rijksbrede implementatiekader inzet van algoritmen), benutten we onze beperkte capaciteit optimaal.

Het op de Douane context toegesneden kwaliteitssysteem ziet er op hoofdlijnen als volgt uit:

Governance, ingericht conform three lines of defence
De bestuurlijke verantwoordelijkheid dient op basis van de risico-indeling van algoritmen op het juiste niveau te zijn belegd. Daarnaast wordt de auditeerbaarheid van algoritmen, en daarmee dus ook de rollen en verantwoordelijkheden gewaarborgd middels een de *three lines of defense* raamwerk:

- De eerste lijn ontwikkelt en/of beheert het algoritme (life-cycle-management), of laat dat doen. Daarnaast dient er sprake te zijn van een aanleiding (risico) dat afgedekt moet worden alvorens te starten met de ontwikkeling van het algoritme. Er moet dus sprake zijn van een kapstok waaraan het algoritme gekoppeld kan worden. De toets hierop valt ook onder de 1e lijn en wordt verwerkt in het systeem DOU-IT
- De tweede lijn doet aan testen en validatie van het model, door te kijken naar de methodische juistheid, data 'footprint', datakwaliteit etc. en checkt ook of de benodigde waarborgen zijn ingeregeld. De tweede lijn maakt op basis van deze tests en validatie de risico's van keuzes uit de eerste lijn duidelijk voor degene die uiteindelijk al dan niet bestuurlijk akkoord dient te geven.
- De derde lijn is die van de audit, waarbij gecontroleerd wordt of de eerste- en tweede lijn hun werk goed gedaan hebben.
- Tot slot is er ook sprake van een vierde lijn van externe audit zoals de recent opgerichte algoritme waakhond en/of ombudsman.

Levenscyclus, met robuuste en gestandaardiseerde processen
Elk algoritme doorloopt de levenscyclus (zie het figuur hieronder) en volgt daarmee gestandaardiseerde robuust ontwikkel-, test- en valideringsprocessen. De gedetailleerde inrichting van deze processen kan afhankelijk zijn van de risico-indeling.



Documentatie en IV-ondersteuning
De documentatie voor de benodigde waarborgen (op risico-indeling) dient op orde te zijn, terug te vinden en deelbaar te zijn. Dit dient ondersteund te worden door marktconforme IV-ondersteuning zoals bijvoorbeeld Gitt.

Transparantie en communicatie
Vanuit de overheid zijn we maatschappelijk verplicht[19] om de benodigde helderheid te geven over de inzet van algoritmen waar de besluitvorming aangaat die burgers of bedrijven raakt. Minimaal voor de hoog risico geclassificeerde algoritmen dient op een voor de burger uitlegbare wijze inzicht te worden gegeven op de inzet ervan middels een algoritmeregister.

5. Beproevingen

Om een beter beeld te krijgen van wat de Douane te doen staat op het gebied van ontwikkeling en implementatie van het kwaliteitssysteem zoals beschreven in hoofdstuk 4 en daarmee de toepasbaarheid van de in hoofdstuk 3 genoemde kaders, heeft de Douane enkele beproevingen uitgevoerd rondom haar fiscale selectieprofielen.

Beschrijving beproeving fiscale selectieprofielen
De beproeving die uit is gevoerd bestaat uit de volgende stappen:
- Stap 1 Inzicht / inventarisatie
  - Totaal aantal fiscale algoritmen
  - Hoeveel van deze fiscale algoritmen bevatten persoonsgegevens
- Stap 2 Risico-indeling volgens Europese AI Act
  - Bepalen of en zo ja welke fiscale algoritmen in de risicogroep “high risk” vallen. Hierbij wordt gebruik gemaakt van de criteria uit het werkdocument dat een eerste basis vormt voor het implementatiekader algoritmen Rijk en een verdieping is van genoemde risico waardering uit de Europese AI Act
  - Welke criteria uit praktijkervaring zijn nog meer gehanteerd om tot een indeling te komen
- Stap 3 Toetsen aan het ADR-normenkader (Governance en GITC)
  - Twee of drie fiscale algoritmen tegen het ADR-normenkader aanhouden. Voor de onderdelen Governance en GITC aangeven hoe aan de gestelde norm is voldaan of aangeven wat er gedaan zou moeten worden om dit te realiseren.
  - Bepalen of er eenvoudig een decompositie valt te maken van de benodigde waarborgen per risiconiveau uit de AI Act
- Stap 4 Toetsen aan het Waarborgenkader MinFin
  - Twee of drie fiscale algoritmen tegen het Waarborgenkader MinFin aanhouden en aangeven of aan de gestelde norm is voldaan.
  - Bepalen of het waarborgenkader past bij de inzet van algoritmen in een organisatie dat zich toespitst op het logistieke proces met bijbehorende data of dat een afgeleide set meer voor de hand ligt.

Uitkomsten beproevingen fiscale selectieprofielen

[19] Algemene beginselen van behoorlijk bestuur

- Stap 1 Inzicht / inventarisatie (zie bijlage 1)
    - Het verkregen overzicht heeft betrekking op actieve profielen die een doorlooptijd hebben vanaf 2008 t/m 29 december 2022. Tijdens de doorlooptijd zijn er *654 selectieprofielen*.
    - In drie gevallen wordt aangegeven dat het risicoprofiel AVG-gevoelige informatie bevat en in zes gevallen is het verzuimd (null) om het desbetreffende vinkje aan te zetten.
    - In de drie gevallen waarin het risicoprofiel AVG-gevoelige informatie is geactiveerd is er sprake van onjuiste toepassing. Bepaalde zelfstandig naamwoorden of familienamen van natuurlijke persoon die als rechtspersoon worden gebruikt worden – in dit geval – als natuurlijkpersoon aangemerkt.
    - In een aantal gevallen worden risico-indicatoren gebruikt zoals: geadresseerde (523 keer), afzender (13 keer) en straatnaam in combinatie met huisnummer (3 keer). In theorie zou dit kunnen betekenen dat deze risico-indicatoren ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is, in deze gevallen gaat het hier om zeer waarschijnlijk rechtspersonen en niet om natuurlijkpersonen. Maar t.b.v. e-commerce is het niet uitgesloten dat in de goederenstroom B2C dan wel C2C wel natuurlijkpersonen in de toekomst zullen worden meegenomen. Vooralsnog wordt in DECO alleen gekeken op basis van de steekproef.
- Stap 2 Risico-indeling volgens Europese AI Act (zie bijlage 1)
    - De fiscale algoritmen die in de beproeving zijn betrokken, kunnen - op basis van de Europese AI-Act – worden geclassificeerd als AI-systemen met een minimaal risico.
- Stap 3 Toetsen aan het ADR-normenkader (Governance en GITC) (zie bijlage 2)
    - Met een beperkte inspanning kan voor de onderdelen Governance en GITC wordt aangeven worden hoe aan de gestelde norm is voldaan of worden aangegeven wat er gedaan zou moeten worden om dit te realiseren.
    - Er kan voor de fiscale risicoprofielen een decompositie worden gemaakt van de benodigde waarborgen per risiconiveau uit de AI Act.
    - Profielen kennen binnen de Douane veelal een uniforme opbouw en maken slechts van een beperkt aantal risico indicatoren op basis van aangiftegedrag gebruik. Hierdoor is het mogelijk om het ADR-normenkader eerst voor het geheel aan fiscale risicoprofielen in één keer te beoordelen en daarna waar nodig specifiek in te zoomen op bepaalde onderdelen.
    - Er zijn weliswaar meerdere verbeterpunten geconstateerd echter over de gehele linie valt op te maken dat de Douane haar zaken zeer behoorlijk op orde heeft en er de afgelopen jaren, mede met de komst van DOU-IT waarin we alles vastleggen, goede kwaliteitsstappen zijn gezet.
- Stap 4 Toetsen aan het waarborgenkader MinFin (zie bijlage 3)
    - Het waarborgenkader MinFin heeft net een andere invalshoek dan het ADR-normenkader gegeven tijdens de beproeving van in gebruik zijnde fiscale risicoprofielen.
    - Uit de beproeving komt naar voren dat het wenselijk is onderscheid te maken tussen eenvoudig en meer complexere algoritmen. Voor de recht toe recht aan profielen betekend deze werkwijze veel tijdverlies, ervanuit gaan dat Fiscaal over ruim 654 eenvoudige algoritmen beschikt.
    - Het blijkt lastig aan te geven of aan de gestelde norm is voldaan vanwege het hoge abstractieniveau van het waarborgenkader MinFin.
    - Het waarborgenkader MinFin schrijft bij bepaalde punten een bepaalde invulling voor (het hoe i.p.v. het wat) die niet altijd passend is voor de Douane.
    - Er zijn meerdere punten die niet over het algoritme gaan maar over het proces.
    - Meerdere punten gaan ervan uit dat er persoonsgegevens gebruikt worden in het algoritme terwijl dit binnen de Douane (domein Fiscaal) over het geheel genomen niet het geval is.

Constateringen vanuit de beproevingen
Op basis van de uitkomsten van de beproevingen komen de volgende aandachtspunten naar voren, kunnen de volgende aanbevelingen gedaan worden en conclusies getrokken worden:

- Zorg waar mogelijk voor een bundeling van algoritmen zoals nu ook voor de fiscale algoritmen is gedaan. Zo zou het kunnen zijn dat alle algoritmen voor het proces kofferselectie tezamen slechts 1x in het algoritmeregister opgenomen hoeven te worden.

- Er wordt binnen de Douane over het geheel genomen geen gebruik gemaakt van persoonsgegevens in onze algoritmen. Maar t.b.v. e-commerce is het niet uitgesloten dat in de goederenstroom B2C dan wel C2C in de toekomst wel natuurlijkpersonen zullen worden meegenomen.
- Werk de governance rond algoritme gebruik verder uit aan de hand van het three lines of defence model zoals ook benoemd in het kwaliteitssysteem.
- De indeling van laag/hoog en eenvoudig/geavanceerd werkt.
- Stel een kort beleidskader op over hoe de Douane wenst om te gaan met de inzet van het algoritmeregister.
- Maak de beproeving van stap 3, toetsen aan het ADR-normenkader, voor fiscale risicoprofielen af en breidt dit uit voor ook de datascience risicodetectie (pillenpilot).
- Laten we de ADR halverwege de implementatie van het kwaliteitssysteem toetsen of we als Douane op de goede weg zijn.
- Herbevestigen dat we als Douane de lijn op landelijk niveau blijven volgen van de brede definitie rond algoritmen.
- Het ADR-normenkader is beter bruikbaar als basiskader voor een Douane waarborgenkader dan het MinFin waarborgenkader. Zo is het ADR-normenkader meer gedetailleerd en levert daarmee scherpere verbetervoorstellen op. Bij onderscheid laag/hoog geldt dat bij eenzelfde wijze van administratie zoals nu bij de fiscale risicoprofielen is gebeurd het een beperkte inzet kost en er voor hoog geclassificeerde algoritmen meer ruimte is om de waarborgen explicieter en steviger in te richten.
- DOU-IT dient voorzien te worden van een uitleg/toelichting met betrekking tot AVG-aspecten. Wanneer wel en wanner niet. Hiermee verkrijgen we meer bewustwording.
- Technisch-profielbeheer beschikt nog niet over de juiste tools om structureel te kunnen testen en valideren van de algoritmen.
- Er dient meer bewustwording te komen vanuit ethische perspectief.
- De maatregelen zouden periodiek gemonitord en geëvalueerd moeten worden.

6. Voorstel aanpak

Binnen de aanpak maken we onderscheid tussen 1) het (verdere) ontwerp van het kwaliteitssysteem 2) de implementatie en 3) in gebruik name ervan.

Hierbij werken we qua tijdslijn toe naar een afronding van de ontwerpfase medio Q3 2023, zodat je daarna nog 1 à 2 jaar hebt om alle algoritmen in scope en compliant te krijgen met alle wettelijke kaders. (alvorens de Europese AI act effectief wordt, maar ook Rijksbrede verplichtingen op dit onderwerp).

Ontwerpfase

1. De ontwerpfase kent twee mijlpalen:
    a. Een, op basis van dit document, overkoepelend ontwerp van het kwaliteitssysteem met daarin een verdere uitwerking van de levenscyclus, gestandaardiseerde processen en documentatie, koppeling van governance aan douanerollen, etc.
    b. Een, voor elke fase in de levenscyclus van het kwaliteitssysteem, de minimale set aan criteria (waarborgen) definiëren waaraan in die stap voldaan (inclusief documentatie) dient te zijn. Dit dient te geschieden voor zowel de hoog- als laag geclassificeerde risicomodellen.

Implementatiefase

2. De implementatiefase is bedoeld om voor elk algoritme de documentatie op orde te krijgen, de processen te doorlopen en te toetsen op opzet en werking, enzovoorts. De implementatiefase gebeurt volgens een iteratief proces waar er steeds wordt geleerd en bijgestuurd om uiteindelijk een optimaal werkend kwaliteitssysteem te creëren. Factoren die hierbij een rol spelen zijn:
    a. Het politieke klimaat om ook voor laag risico geclassificeerde algoritmen een brede set aan waarborgen te verplichten. Hiervoor kan samenwerking gezocht worden met overheidsorganisaties die zich in meer vergelijkbare context begeven zoals het RVO, RWS en NVWA alsook andere Europese douaneorganisaties.
    b. Het aantal algoritmen waarbij een mogelijke onderverdeling in hoofd- en sub-modellen van grote invloed is.
    c. Het aantal hoog risico geclassificeerde algoritmen binnen de Douane.
    d. Ontwikkelingen als bijvoorbeeld een Rijks- of Ministerieel-breed algoritmeregister waarop aangesloten kan worden.

3. De ingebruikname betekent ook enkele "nieuwe" werkzaamheden zoals het opkomen voor de douanebelangen in de Europese en Rijksbrede ontwikkelingen op het gebied van algoritmen, waarbij nadrukkelijk de samenwerking wordt gezocht met partijen die zich in een meer vergelijkbare context begeven. Maar ook op het gebied van auditen, communicatie en transparantie brengen extra werkzaamheden met zich mee.

Tijdschatting

- Ontwerpfase: voor een organisatie met de complexiteit, staat van borging en het algoritmegebruik van de Douane kost het ontwerp naar schatting driekwart jaar (gezien bij vergelijkbare instellingen), uitgaande van 2 tot 3 FTE, deels belegd bij reeds bestaande functies. In workshops met betrokkenen vinden ontwerp en documentatie plaats (van de governance op hoofdlijnen tot bijvoorbeeld een document met gedetailleerde instrumenten die elke model ontwikkelaar in de ontwikkelfase moet toepassen om de ethische toepassing te waarborgen).

- De implementatiefase, kent twee stromen ,
  a. Implementatie van het algehele kwaliteitssysteem voor de generieke componenten, waaronder bijvoorbeeld de inrichting van een algoritme register, trainingen, communicatiestrategie etc. Dus componenten die niet of nauwelijks afhankelijk zijn van het aantal algoritmes
  b. Implementatie, op basis van risico classificatie, van de set aan waarborgen voor elk (hoofd)algoritme met daarbij mogelijke bijlagen voor de hiervan afgeleide sub-modellen.

- Bij vergelijkbare organisaties wordt de ontwerpfase en stap "a" van de implementatiefase een afgerond geheel beschouwd. Stap "b" van de implementatie moet idealiter in de lijn plaatsvinden en geleidelijk bij zowel nieuwe en bestaande algoritmes (e.g. voor elk algoritme moet je op een gegeven moment zorgen dat je de levenscyclus bent doorlopen). Hiervoor is de hierboven genoemde 1 a 2 jaar nodig gegeven de doorlooptijd van de levenscyclus en aantal algoritmen

Mijlpalenplanning en benodigde expertise

Benodigde expertise
Implementatiemanager
Kwaliteitsmanagement DLTC
Datascience medewerker
HHB wettelijke grondslagen uitvoeringsprocessen
IM/BIS expertise
Communicatiespecialist
CIO/CDO Office