

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

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.

Officiëren 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 fasen en eventueel een 'safe harbor' of experimenteeromgeving? • Op welke wijze wordt het resultaat van het project gebruikt? Wordt het in de operatie (kan gaan om alle fasen 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
---------------------------------	---	---	--

	- o Wat doet het met de data (parametrisering) - o Wat komt er uit (selectie, patroon)? - o 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