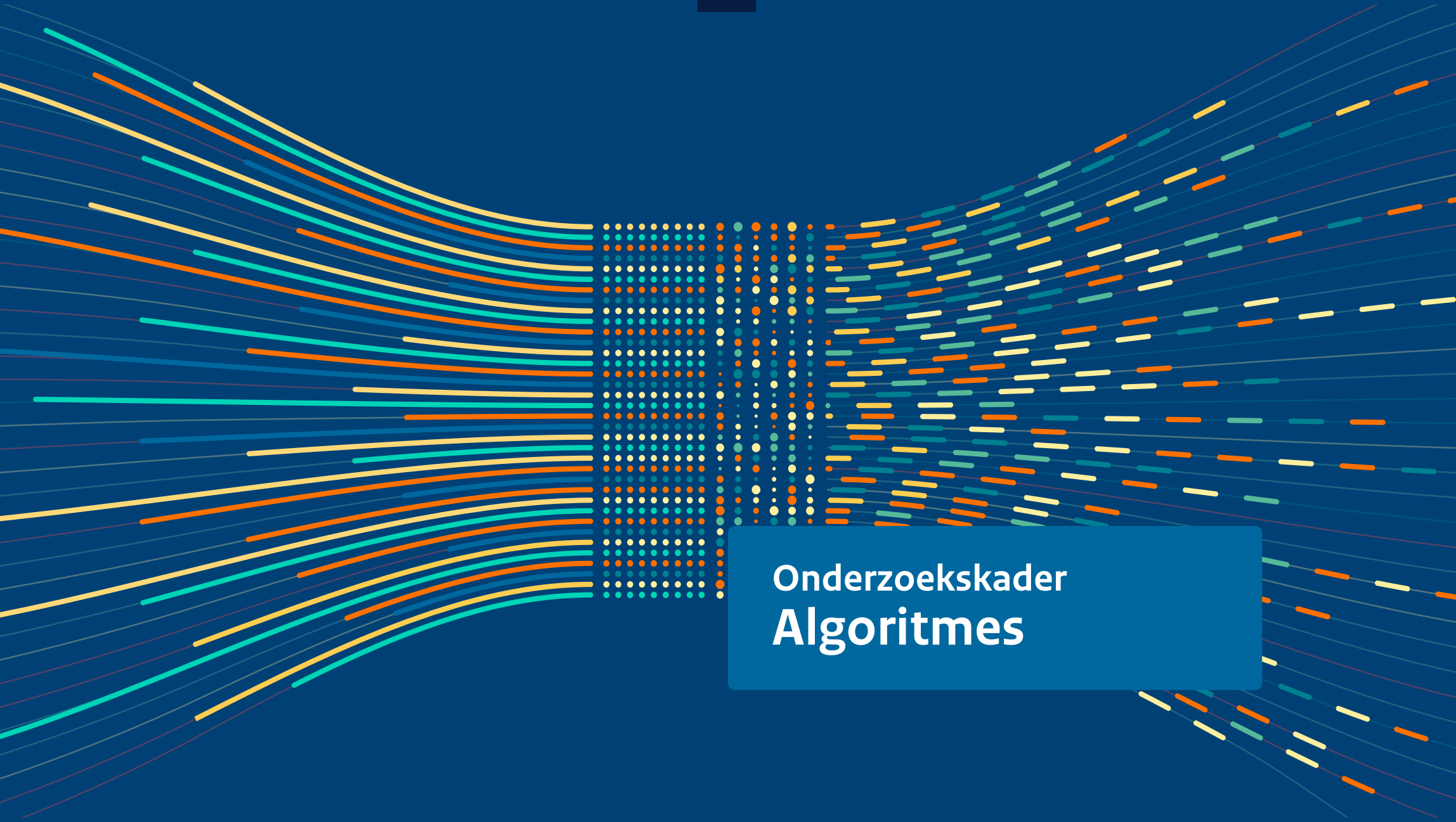
Auditdienst Rijk
*Ministerie van Financiën*



# Onderzoekskader
# Algoritmes

# Inhoudsopgave

# Introductie

*Dit onderzoekskader is een instrument om de beheersing van algoritmes in kaart te brengen. Het geeft inzicht in de risico's die algoritmes met zich meebrengen en met welke maatregelen deze risico's beheerst (kunnen) worden.*

### *Voor wie*

Het onderzoekskader is in eerste instantie bedoeld als instrument voor auditors om de beheersing en werking van algoritmes binnen overheidsorganisaties te onderzoeken, maar is ook bruikbaar voor andere partijen om inzicht te krijgen in de huidige en/of gewenste beheersing van algoritme(s).

### *Reikwijdte*

Het kader richt zich op algoritmes die binnen overheidsorganisaties gebruikt worden. Het is ingericht op algoritmes die zelf van voorbeelden leren, zoals machine learning, maar is ook toepasbaar op regelgebaseerde algoritmes. Het kader is ook bruikbaar voor andere organisaties en kan bij verschillende fases van de levenscyclus van een algoritme worden ingezet. Mogelijk zijn niet alle thema's relevant gezien de context van het algoritme. De opdrachtgever en auditor(s) dienen daarom voorafgaand aan een onderzoek te analyseren en te bepalen welke thema's en onderwerpen worden onderzocht. Het onderzoekskader is ingedeeld in **4 thema's**:

- Sturing & Verantwoording
- Privacy
- Data & Model
- Informatiebeveiliging

Ethiek raakt alle thema's en komt daarom bij elk thema in het kader terug. Elk thema bevat deelgebieden en de risico's en beheersmaatregelen die daarbij horen (inclusief de bron).
Ook deze kunnen weer gerelateerd zijn aan een ander thema. Een apart werkbestand voor auditors is opgesteld wat kan worden gebruikt bij het uitvoeren van een onderzoek. Dit bestand heeft dezelfde opbouw, maar bevat ook invulvelden om als auditor het risico (kans x impact) in te schatten en de bevindingen op te nemen. Daarnaast zijn toelichtingen en voorbeelden van checks & evidence opgenomen per beheersmaatregel.

### *Relatie andere richtlijnen en kaders*

Het onderzoekskader is ontwikkeld met behulp van nationale en internationale richtlijnen en kaders, rapporten en instrumenten, zoals de Ethics guidelines for trustworthy AI van de Europese Commissie (EC), Impact Assessment voor Mensenrechten bij de inzet van Algoritmes (IAMA), de richtlijnen van het ministerie van JenV, het DPIA model rijksoverheid (gebaseerd op o.a. AVG) en de Guiding Principles Trustworthy AI Investigations van NOREA (beroepsvereniging IT-auditors Nederland). De bron van de betreffende risico's en beheersmaatregelen is tevens opgenomen.

# 1 Sturing en verantwoording

*Beheersdoelstelling*

***De doelstelling, impact en risico's van het algoritme zijn geïnventariseerd en beoordeeld en passende maatregelen zijn getroffen om ongewenste effecten te voorkomen. Het gebruik van het algoritme is transparant en conform wet- en regelgeving en intern beleid. De rollen en verantwoordelijkheden van betrokkenen zijn belegd voor een adequate sturing en verantwoording. De organisatie evalueert periodiek de naleving van de maatregelen en de kwaliteit van het algoritme.***

*Risico*

De sturing en verantwoording t.a.v. het algoritme is niet adequaat. De doelstelling, impact, risico's en kwaliteit van het algoritme zijn niet (periodiek) beoordeeld en passende maatregelen ontbreken, wat kan leiden tot ongewenste effecten zoals discriminatie. Het gebruik van het algoritme is niet transparant en conform wet- en regelgeving en intern beleid.

*Prepared By Client (PBC)*

- Documentatie van gemaakte afwegingen en keuzes (zoals IAMA)
- Functionele documentatie/ontwerp
- Technische documentantie/ontwerp
- Interne toets naleving wet- en regelgeving/intern beleid
- Goverancebeschrijving en bewijs van bestaan/uitvoering
- Risicoanalyse- en rapportage
- Documentatie over transparantie naar doelgroep over gebruik algoritme
- Procesbeschrijvingen en bewijs van bestaan/uitvoering (bij diverse beheersmaatregelen)
- Evaluatierapportage(s)
- Overeenkomst met externe partij (indien van toepassing)

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Doelstelling*** | Het algoritme dient niet het beoogde doel en onderliggend probleem. Zonder eenduidigheid over het doel is geen sturing op en verantwoording over het algoritme mogelijk. | SV.1 | Het probleem bij de taakuitvoering wat met de inzet van het algoritme moet worden opgelost is geïnventariseerd. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1 en 1.7 |
| | | SV. 2 | Een bewuste afweging of het algoritme het juiste middel is om het probleem op doelmatige en doeltreffende wijze op te lossen is gemaakt en vastgelegd. | EC/AI HLEG April 2019 - Hoofdstuk II.1.7 |
| | | SV.3 | De doelstelling van het algoritme is helder en vastgelegd. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1 en 1.7 |
| ***Impact*** | De impact van het algoritme op de besluitvorming en op personen, doelgroepen en/of de samenleving is niet inzichtelijk, waardoor onvoldoende maatregelen zijn getroffen om ongewenste effecten (zoals bias en discriminatie) te voorkomen. | SV.4 | De impact van het algoritme is geïnventariseerd en beoordeeld. | EC/AI HLEG April 2019 - Hoofdstuk I. 1.1 & Hoofdstuk II. 1.6 |
| | | SV.5 | Indien het algoritme leidt tot geautomatiseerde besluitvorming dan wel anderszins een aanmerkelijke impact heeft, is bepaald of menselijke tussenkomst noodzakelijk of wenselijk is. Dit is in het proces ingeregeld. | EC/AI HLEG April 2019 - Hoofdstuk II.1.4 |
| | | SV.6 | De gebruiker is in staat een betekenisvolle rol bij de besluitvorming te vervullen. Het besluit om de uitkomst van het algoritme te volgen wordt niet beïnvloed door (externe) factoren. | EC/AI HLEG April 2019 - Hoofdstuk II.1.1 |
| ***Wet- en regelgeving en beleid*** | Het algoritme en beoogde besluiten voldoen niet aan wet- en regelgeving en intern beleid en kaders. | SV.7 | Voor de inzet van het algoritme en de beoogde besluiten die genomen zullen worden op basis van het algoritme is een wettelijke grondslag. | Algemeen |
| | | SV.8 | Het algoritme voldoet aan de intern vastgestelde beleidskaders. | Algemeen |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Betrokkenen en verantwoordelijkheden*** | De sturing en verantwoording is ontoereikend en niet geborgd. Onvoldoende betrokkenheid van belanghebbenden en onvoldoende capaciteit en deskundigheid in de organisatie vergroot de kans op fouten en ongewenste effecten. | SV.9 | De rollen en verantwoordelijkheden bij de ontwikkeling en inzet van het algoritme zijn belegd. | Algemeen |
| | | SV.10 | Relevante belanghebbenden zijn bij de ontwikkeling en inzet van het algoritme betrokken. | EC/AI HLEG April 2019 - Hoofdstuk II.1.5 |
| | | SV.11 | Indien het algoritme is ontwikkeld door een externe partij, zijn er heldere afspraken gemaakt, o.a. over eigenaarschap, beheer, prestatiecriteria en reproduceerbaarheid van het algoritme. | EC/AI HLEG April 2019 - Hoofdstuk II.1.7 |
| | | SV.12 | De capaciteit en deskundigheid bij de ontwikkeling en inzet van het algoritme is toereikend. | Algemeen |
| ***Risicomanagement*** | Risico's worden niet (tijdig) vastgesteld en adequaat geadresseerd en behandeld. | SV.13 | Risicomanagement vindt gestructureerd plaats vooraf en tijdens de inzet van het algoritme. | Algemeen<br>EC/AI HLEG April 2019 - Hoofdstuk II.1.7 |
| ***Transparantie*** | Belanghebbenden hebben geen inzicht in de inzet van het algortime, wat het algoritme doet en welke consequenties dit heeft. | SV.14 | De inzet en werking van het algoritme is gepubliceerd en inzichtelijk voor de doelgroep. De mate van transparantie en uitlegbaarheid daarbij is afgewogen. | EC/AI HLEG April 2019 - Hoofdstuk II.1.4 |
| | | SV.15 | Maatregelen om besluiten genomen door of aan de hand van het algoritme te herleiden en/of te herbeoordelen zijn aanwezig. | EC/AI HLEG April 2019 - Hoofdstuk II.1.2 en 1.4 |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Evaluatie & verantwoording*** | Zonder evaluatie van de kwaliteit van het algoritme is er geen goede sturing, beheersing en verantwoording mogelijk over de inzet van het algoritme. | SV.16 | Een proces voor een periodieke evaluatie van de kwaliteit van het algoritme is gedocumenteerd en in werking. De resultaten worden met belanghebbenden gedeeld. | EC/AI HLEG April 2019 - Hoofdstuk II.1.2 |
| | | SV.17 | De organisatie analyseert of (interne en externe) klachten en incidenten het gevolg kunnen zijn van het gebruik van het algoritme. | EC/AI HLEG April 2019 - Hoofdstuk II 1.7 |
| | | SV.18 | Een procedure om de inzet van het algoritme veilig stop te zetten in het geval dit niet lang wenselijk blijkt, is aanwezig. | EC/AI HLEG April 2019 - Hoofdstuk II.1.2 |
| | | SV.19 | De verantwoordelijke legt verantwoording af over de ontwikkeling, inzet en werking van het algoritme. | EC/AI HLEG April 2019 - Hoofdstuk II.1.7 |

# 2 Privacy

*Beheersdoelstelling*

***De kenmerken en rechtmatigheid van de verwerking van de persoonsgegevens en de privacyrisico's zijn beoordeeld en passende maatregelen zijn getroffen om de risico's te mitigeren. De gegevensverwerking door een algoritme is transparant voor de betrokkenen en zij hebben de mogelijkheid om hun rechten uit te oefenen. De verwerking door algoritme is in overeenkomst met de privacywetgeving (AVG).***

*Risico*

De verwerking van persoonsgegevens is niet proportioneel/substantieel en rechtmatig. Privacyrisico's worden niet (tijdig) gesignaleerd en/of passende maatregelen ontbreken, waardoor persoonsgegevens niet adequaat beschermd worden en kan leiden tot schade voor de betrokkene. Wanneer de verwerking door een algoritme niet transparant is voor betrokkenen, hebben zij geen controle over hun gegevens en kunnen ze geen beroep doen op hun privacyrechten.

*Prepared By Client (PBC)*

- Risicoanalyse- en rapportage (DPIA)
- Opvolging voorgenomen maatregelen n.a.v. rapportage (DPIA)
- Functionele en technische documentatie/ontwerp
- Documentatie over transparantie naar doelgroep over gebruik algoritme
- Procesbeschrijving en bewijs inrichting/uitvoering van rechten van betrokkenen en bewaartermijn

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Verwerkingsverantwoordelijke*** | Sturing en verantwoording is niet helder en ontbreekt daardoor. | PRI.1 | De verwerkingsverantwoordelijke en verwerker van de persoonsgegevens die het algoritme verwerkt zijn vastgesteld. | AVG, art. 24,26,27, 28,29. |
| ***DPIA*** | Inzicht in privacyrisico's ontbreekt. | PRI.2 | Een risicoanalyse (indien noodzakelijk een DPIA) met de nodige diepgang en substantie is uitgevoerd om privacyrisico's in kaart te brengen. | AVG, art. 35. |
| | Er zijn geen maatregelen getroffen om de geïnventarsieerde risico's te mitigeren. | PRI.3 | Passende maatregelen op basis van de gesignaleerde privacyrisico's zijn aanwezig. Deze maatregelen zijn zo veel mogelijk bij de ontwerpfase getroffen (privacy by design). | AVG, art. 35. |
| ***Doeleinde*** | Het doel is onduidelijk waardoor de verwerking van persoonsgegevens niet bijdraagt aan het doel van het algoritme. | PRI.4 | Het doel van de verwerking van persoonsgegevens door het algoritme is welbepaald en omschreven. | AVG, art. 5. |
| ***Data-minimalisatie*** | De verwerkte gegevens zijn niet proportioneel en relevant in relatie tot het doel. | PRI.5 | Het algoritme verwerkt niet meer persoonsgegevens verwerkt dan noodzakelijk; de verwerkte gegevens zijn proportioneel en substantieel. | AVG, art. 5. |
| ***Rechtmatige grondslag*** | De verwerking van de persoonsgegevens met het algoritme is onrechtmatig. | PRI.6 | De verwerking van persoonsgegevens door het algoritme heeft een rechtmatige grondslag. | AVG, art 6. |
| ***Persoonsgegevens*** | Het algoritme verwerkt (onbewust) persoonsgegevens die het niet mag verwerken. | PRI.7 | De persoonsgegevens en bijzondere en strafrechtelijke persoonsgegevens die het algoritme verwerkt zijn geïdentificeerd. | AVG, art. 9, 10. |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Transparantie*** | Betrokkenen zijn niet op de hoogte dat hun persoonsgegevens worden verwerkt middels een algoritme, waardoor zij geen controle hebben. | PRI.8 | De betrokkenen zijn geïnformeerd over de verwerking van persoonsgegevens door het algoritme en de verwachte gevolgen. | AVG, art. 12-14. |
| ***Rechten van betrokkenen*** | Betrokkenen hebben geen controle over hun persoonsgegevens doordat ze geen beroep kunnen doen op hun privacyrechten. | PRI.9 | Een proces om gehoor te geven aan de rechten van betrokkenen is aanwezig en ingeregeld. | AVG, art. 15-21. |
| ***Besluitvorming*** | De betrokkene ondervindt aanmerkelijke gevolgen door een geautomatiseerd besluit. | PRI.10 | Het algoritme betreft geen uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor de betrokkene juridische of anderszins aanmerkelijke gevolgen zijn verbonden. | AVG, art. 22. |
| ***Bewaartermijnen*** | Persoonsgegevens worden langer bewaard dan nodig. | PRI.11 | De persoonsgegevens die het algoritme verwerkt worden niet langer bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is.<br>Zij worden tijdig vernietigd conform procedure. | AVG, art. 5.<br>Archiefwet. |

# 3 Data & Model



*Beheersdoelstelling*

***De input-, training- en testdata zijn representatief. De betekenis en herkomst van inputdata zijn eenduidig interpreteerbaar. De data is juist en consistent. Maatregelen zijn getroffen om vervuiling van inputdata tegen te gaan. De prestatie van het model is in overeenkomst met de voor het algoritme gestelde eisen. Deze eisen volgen uit de functie die het algoritme in het proces waarbinnen het gebruikt wordt vervult. De ethische overweging over het gewenst handelen en de uitkomsten van het algoritme zijn gemaakt. Het algoritme is eerlijk voor de beschermde subpopulaties en individuen volgens de uit de ethische overweging volgende definitie van eerlijkheid. Het model is controleerbaar en de uitkomsten zijn reproduceerbaar.***

*Risico*

De prestatie van het model is niet in overeenstemming met de vereisten die voor het model gelden. Het model creëert onwenselijke systematische afwijking voor specifieke personen, groepen of andere eenheden. De werking en uitkomst van het algoritme past niet bij de voor het proces opgestelde definitie van eerlijkheid en wenselijkheid. De uitkomsten van het algoritme zijn niet reproduceerbaar.

*Prepared By Client (PBC)*

- Prepared By Client (PBC)
- Functionele documentatie/ontwerp
- Technische documentatie/ontwerp
- Definition of succes/prestatiecriteria
- Risicoanalyse- en rapportage
- Exploratieve data-analyse (EDA)
- Data model/glossarium
  Biasanalyse
- Overeenkomst met externe partij (indien van toepassing)
- Evaluatierapportage(s) (zoals peer review of toets modelprestatie)

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Doelstelling*** | Algoritme functioneert niet in lijn met geformuleerde doelstellingen. | DM.1 | De doelstelling van het algoritme is concreet uitgewerkt tot functionele eisen voor het algoritme. De mate waarin aan deze eisen is voldaan is bepaald. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1 t/m 1.6 |
| ***Prestatie*** | Het model presteert suboptimaal voor de taak die uitgevoerd moet worden. | DM.2 | De keuze voor het model en de hyperparameters zijn beargumenteerd en vastgelegd. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.2 |
| | Het model wordt toegepast terwijl niet aan de voorwaarden voor het model voldaan wordt. Prestatie zoals op de testset is niet gegarandeerd. | DM.3 | De grenzen van de toepasbaarheid van het model zijn gedocumenteerd. De voorwaarden waaronder het model gebruikt kan worden en waaronder niet, zijn duidelijk. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1, 1.2 |
| | Bij het in productie nemen van het model of bij latere evaluatie is het niet duidelijk of het model voldoende presteert. | DM.4 | De functionele eisen zijn uitgewerkt tot adequate en meetbare prestatiecriteria. De gestelde criteria zijn behaald. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1 t/m 1.6 |
| | De prestatie van model lijkt hoger dan het in werkelijkheid is. | DM.5 | De train-, test- en validatieset zijn gescheiden. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.2, 2.1§100 |
| | Door onjuiste training van het model presteert het model in de praktijk minder goed dan bij de tests. | DM.6 | Bij de keuze voor training- en testdata in de ontwikkelfase is gelet op under- en overfitting. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.2, 2.1§100 |
| | Het model presteert in productie niet goed door niet representatieve trainings-/testdata. | DM.7 | De doelpopulatie is vastgesteld. Er is gecontroleerd dat de testdata representatief is voor de data van de verschillende subgroepen die in de productiedata voorkomen. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.2, 2.1§100 |
| | Door veranderingen in de data presteert het model niet meer zoals verwacht. | DM.8 | De output en performance van het model worden geëvalueerd bij veranderingen in de data. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.2, 1.3 |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Volledigheid en betrouwbaarheid*** | Door onjuiste interpretatie van gegevens worden verkeerde beslissingen genomen. | DM.9 | De input- en outputdata voldoen qua kwaliteit, volledigheid en betrouwbaarheid aan de functionele eisen. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.3 |
| ***Uitlegbaarheid*** | Gebruikers van het model interpreteren of gebruiken de resultaten van het model verkeerd. | DM.10 | De documentatie over het model (ontwerp, werking en voorwaarden) is bekend en begrijpelijk voor de gebruikers. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1 |
| | De werking van het algoritme wordt foutief uitgelegd. | DM.11 | Bij het gebruik van explainable AI (uitlegbaarheidsalgoritmes) is gecontroleerd of deze betrouwbaar zijn. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.4, 2.1§99 |
| ***Begrijpelijkheid*** | Beslissingen worden genomen op basis van outputdata die verkeerd begrepen zijn, omdat outputvariabelen een andere betekenis hebben dan verwacht. | DM.12 | De outputvariabelen zijn eenduidig interpreteerbaar. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.4 |
| ***Reproduceerbaarheid*** | Het productiemodel is niet te reproduceren door missende trainingsdata. | DM.13 | De trainingsdata is gearchiveerd. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.7 |
| | Waarom het algoritme voor een specifiek individu tot een bepaalde uitkomst heeft geleid is niet na te gaan. | DM.14 | Iedere individuele output is met behulp van hetzelfde model en dezelfde inputdata te reproduceren. Eventuele verschillen zijn verklaard vanuit de modeleigenschappen. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.7 |
| ***Actualisatie na externe wijzigingen*** | Door wijzigingen in de wet- en regelgeving worden de eisen die aan het model zijn gesteld niet meer gehaald. | DM.15 | Wanneer wijziging van wet- en regelgeving aanpassingen in het model vereist, zijn deze doorgevoerd. | Algemeen |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Bias en discriminatie*** | Het model creëert onwenselijke systematische afwijking voor specifieke personen, groepen of andere eenheden (bias/discriminatie) | DM.16 | De definitie van de verschillende groepen en de gewenste prestatie van het model voor deze groepen zijn opgenomen in de functionele eisen. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | | DM.17 | De mate van geaccepteerde bias in de uitkomst is opgenomen in de functionele eisen en uitgewerkt in meetbare prestatiecriteria. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | | DM.18 | De methoden om bias te voorkomen, detecteren en corrigeren zijn vastgelegd. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | | DM.19 | De mate van bias in de data, dataverzameling en het model zijn in kaart gebracht. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | | DM.20 | Tijdens de ontwikkeling van het model is beoordeeld of er een verschil bestaat tussen de prestatie van het model tussen verschillende subgroepen. De prestatiemetrieken afleidbaar uit de confusionmatrix zijn vergeleken voor deze subgroepen. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | | DM.21 | De uitkomstbias van productiedata is beoordeeld voor de verschillende subgroepen en voldoet aan de prestatiecriteria. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.5 |
| | Bias in het algoritme leidt tot discriminatie. | DM.22 | Bij de geconstateerde bias is beoordeeld of deze op discriminatie duidt. | EC/AI HLEG April 2019 - Hoofdstuk II. 1.1, 1.5 |
| ***Afhankelijkheid*** | De organisatie is afhankelijk voor de data of het model afhankelijk van derden en kan daardoor reproduceerbaarheid en prestatie niet garanderen. | DM.23 | De organisatie heeft volledige controle of eigenaarschap over de data. Wanneer dit niet mogelijk is, zijn afspraken gemaakt om de functionele eisen te waarborgen. | EC/AI HLEG April 2019 Hoofdstuk II 1.7 |
| ***Milieu*** | De impact van het model op het milieu is disproportioneel hoog. | DM.24 | De impact van het model op het milieu tijdens de ontwikkeling en bij gebruik is nader geïnventariseerd en is meegenomen bij de modelkeuze. | EC/AI HLEG April 2019 Hoofdstuk II 1.6 |

# 4 Informatiebeveiliging

*Beheersdoelstelling*

***Het beheer op wijzigingen, wachtwoorden, gebruikers en de beveiliging van componenten voorkomt oneigenlijke toegang tot de IT-systemen die gebruikt worden bij het algoritme. Loginformatie wordt bewaard zodat gebruikeractiviteiten kunnen worden achterhaald. Procedures zijn aanwezig om te zorgen dat beveiligingsincidenten zo spoedig mogelijk worden opgepakt. Back-up en recovery beleid en maatregelen zijn aanwezig om te zorgen dat bij uitval van de systemen het algoritme, de data en uitkomsten van het algoritme nog beschikbaar zijn. De informatiebeveiliging is bij het ontwerp opgenomen (security by design) en ook bij uitbesteding aan een leverancier zijn beveilgingsmaatregelen opgelegd.***

*Risico*

Het beheer op wijzigingen, wachtwoorden, gebruikers en de beveiliging van componenten is niet op orde waardoor oneigenlijke toegang, wijziging of vernietiging plaats kan vinden in de IT-systemen. Het algoritme, de data en uitkomsten van het algoritme kunnen daardoor niet meer beschermd en betrouwbaar zijn. Zonder loginformatie is niet te achterhalen wanneer er aanpassingen zijn gedaan bij het algoritme. Gebrek aan security by design en beveiligingseisen voor de leverancier maakt de informatiebeveiliging kwetsbaarder.

*Prepared By Client (PBC)*

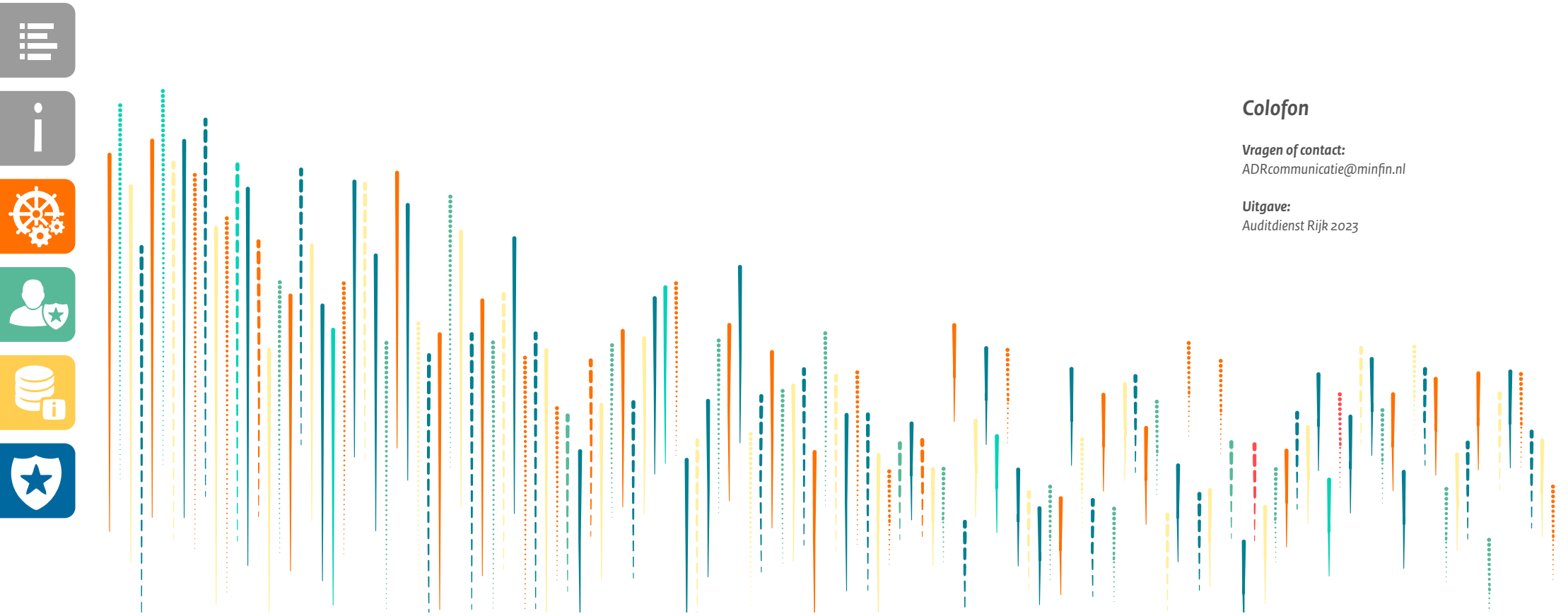
- Lijst met systeemwijzigingen en testverslagen
- Autorisatiematrix en beschrijving rollen/rechten per systeem(laag)
- Lijst met wijzigingen rollen en bijbehorende goedkeuringen
- Overzicht aantallen en rechten per (systeem)laag
- Logfiles
- (Verslag) systeeminstellingen
- Implementatiebewijs twee-factor authentificatie
- Architectuur plaat, security scan, patch overzicht
- Procesbeschrijving back-up and recovery en testenverslagen

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Wijzigings-beheer*** | Er vinden onbedoelde of ongeautoriseerde wijzigingen aan het algoritme of de uitkomsten van het algoritme plaats. | IB.1 | Wijzigingen dienen van te voren te zijn geautoriseerd door de systeemeigenaar of product owner | BIO 12.1.2 |
| | | IB.2 | Wijzigingen worden getest in een andere omgeving dan de productieomgeving. | BIO 12.1.4, 14.2.3, 14.2.9, 14.3.1 |
| | | IB.3 | Wijzigingen worden door de systeemeigenaar of product owner goedgekeurd op basis van gedocumenteerde testresultaten en pas daarna doorgevoerd in de productieomgeving. | BIO 12.1.2, 14.2.2, 14.2.9 |
| | | IB.4 | Er dient functiescheiding te zijn ingericht tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen om onbevoegde en onbedoelde wijzigingen te beperken. | BIO 6.1.2, 14.2.2 |
| | | IB.5 | Er dient periodiek controle plaats te vinden op wijzigingen aan het systeem, zodanig dat oneigenlijke wijzigingen worden gesignaleerd. | BIO 9.4.4, 12.4.1 |
| ***Wachtwoord-beheer*** | Er vindt oneigenlijke toegang plaats tot het algoritme of uitkomsten van het algoritme doordat het wachtwoord te eenvoudig is. | IB.6 | Alle wachtwoorden van gebruikers en beheerders dienen periodiek te worden gewijzigd, met een maximum van 1 jaar. | BIO 9.4.3 |
| | | IB.7 | Voor toegang vanuit een onvertrouwde omgeving dient, twee-factor authenticatie te worden gebruikt. | BIO 9.4.2.1 |
| | | IB.8 | Na een periode van maximaal 15 minuten inactiviteit dient de toegang tot de applicatie te worden vergrendeld en na 10 foutieve inlogpogingen dient het account geblokkeerd te worden. | BIO 11.2.9<br>BIO 9.4.3 |
| | | IB.9 | Wachtwoorden mogen niet in originele vorm (plaintext) worden opgeslagen, maar dienen versleuteld te worden. | NIST 5.1.1.2 |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Gebruikersbeheer*** | Onbevoegde gebruikers hebben toegang tot het algoritme, data of uitkomsten van het algoritme. | IB.10 | Gebruikers en beheerders krijgen slechts toegang tot functionaliteit (rol) die zij uit hoofde van hun functie nodig hebben (need to know, need to use). Daartoe is een beschrijving beschikbaar welke rollen en rechten per applicatie bij een functie horen. | BIO 6.1.2, 9.2.2 en 9.4 |
| | | IB.11 | Het verlenen en muteren van accounts en toegangsrechten vindt plaats na goedkeuring door een bevoegde functionaris. Dit aan de hand van een actueel mandaatregister waaruit blijkt welke personen beslissende bevoegdheden hebben voor het verlenen van een bepaald type (niveau) toegangsrechten danwel functieprofielen. | BIO 9.2.1.2, 9.2.2.1, 9.4 |
| | | IB.12 | Er bestaat functiescheiding tussen het aanvragen, autoriseren en doorvoeren van wijzigingen in gebruikersaccounts en toegangsrechten. | BIO 9.2.1.2, 9.2.2.1, 9.2.3 |
| | | IB.13 | Functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen. | BIO 9.2.2, 9.2.6 |
| | | IB.14 | Het aantal accounts met verhoogde rechten is beperkt en verklaard, en staat in logische verhouding tot de beheerders en of ICT-afdeling. | BIO 9.1.2.(1), 9.2.3, 9.2.4 |
| | | IB.15 | Gebruikersaccounts en beheeraccounts dienen altijd persoonsgebonden en verklaard te zijn, zodat handelingen altijd te herleiden zijn naar één verantwoordelijke. | BIO 9.1, 9.4.2 |
| | | IB.16 | Eindgebruikers hebben geen directe toegang tot de onderliggende componenten (zoals de database). | BIO 9.2.3, 13.1.3 |
| | | IB.17 | Toegangsrechten op onderliggende componenten dienen periodiek, minimaal jaarlijks, geëvalueerd te worden. Dit interval dient te zijn beschreven in het toegangsbeleid en zijn bepaald op basis van het risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd. | BIO 9.2.5 |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Beveiliging van componenten*** | Oneigenlijke toegang van buitenaf vindt plaats via zwakheden in het systeem. | IB.18 | Er is een accuraat inzicht in de beoogde opzet van de IT-infrastructuur (de architectuur) en een actueel inzicht in de werkelijk geconfigureerde hard- en software. | CIS Control 1<br>BIO 8.1.1 |
| | | IB.19 | Er is formeel een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal periodieke (geautomatiseerde) controle op de aanwezigheid van kwetsbaarheden in de te toetsen systemen, een risicoafweging en navolgbare afwerking daarvan of risicoacceptatie. | BIO 12.6 |
| | | IB.20 | Zodra kwetsbaarheden bekend zijn dienen de te beoordelen IT-systemen tijdig te worden gepatched en geupdated. | BIO 12.6.1 |
| | | IB.21 | Softwarecomponenten en services die niet noodzakelijk zijn voor het functioneren van het algoritme zijn verwijderd of gedeactiveerd om beveiligingsrisico's te beperken. | BIO 12.6.1 |
| | | IB.22 | Zonering binnen de technische infrastructuur vindt plaats conform de uitgangspunten die zijn vastgelegd in een operationeel beleidsdocument, waarbij minimaal sprake is van scheiding tussen vertrouwde en onvertrouwde netwerken. | BIO 9.4.3 |
| | | IB.23 | Actieve monitoring van de algoritme data vindt plaats zodat beveiligingsincidenten en -gebeurtenissen in een vroeg stadium worden gedetecteerd. | BIO 12.4.1<br>NCSC Handreiking voor implementatie van detectieoplossingen |
| | | IB.24 | Het interne netwerk is gescheiden van andere onvertrouwde omgevingen | BIO 13.1.3 |
| | | IB.25 | Netwerkverkeer en componenten worden actief gemonitord. | BIO 12.4.1 |

| Deelgebied | Risico | # | Beheersmaatregelen | Bron |
|---|---|---|---|---|
| ***Back-up en Recovery*** | Er is geen hersteloptie bij uitval van het algoritme en er is risico van gegevensverlies. | IB.26 | Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. De back-ups worden gemaakt, bewaard en getest conform beleid. | BIO 12.3.1.1, 12.3.1.4, 12.3.1.5 |
| ***Logging*** | Zonder loginformatie is niet te achterhalen wanneer er aanpassingen zijn gedaan (audit trail) op (de code van) het algoritme. | IB.27 | Loginformatie wordt bewaard en is toegankelijk totdat de bewaartermijnen zijn verstreken. | BIO 12.4.1.1, 12.4.2.2 |
| ***Security by design*** | Indien de opzet en inrichting niet voldoet aan vastgestelde security by design principeskan dit leiden tot oneigenlijke toegang, wijzigingen of vernietigingen van het algoritme, de data of uitkomsten. | IB.28 | Security by design is gehanteerd en terug te zien als uitgangspunt. | BIO 14.2.1.1 |
| ***Leveranciersrelaties*** | Indien de (externe) leverancier beveilingseisen niet op orde heeft, is het risico op inbreuk op BIV van het algoritme en/of data aanwezig. | IB.29 | Bij uitbestedingstrajecten dient er een expliciete risicoafweging te zijn. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd. | BIO 15.1.1.1 |
| ***Beheer van informatiebeveiligingsincidenten*** | Te late reactie kan zorgen dat de BIV van het algoritme en of data kan worden aangetast. | IB.30 | Er zijn procedures aanwezig die borgen dat beveiligingsincidenten m.b.t. algoritmes en data zo spoedig mogelijk, afhankellijk van de kwalificatie van het incident, worden opgepakt. | BIO 16.1.1, 16.1.5 |



## Colofon

***Vragen of contact:***
*ADRcommunicatie@minfin.nl*

***Uitgave:***
*Auditdienst Rijk 2023*