# Algoritmes getoetst

De inzet van
9 algoritmes bij
de overheid

2022

Algemene
Rekenkamer

# Inhoud

# 1. Samenvatting

Elke maand neemt de overheid miljoenen beslissingen. Bijvoorbeeld over wie wel en wie geen huurtoeslag krijgt. Of wie een boete moet krijgen voor te hard rijden. Voor al die beslissingen gebruikt de overheid algoritmes. Een algoritme is een reeks van opdrachten die een computer volgt. Daarmee wordt een probleem opgelost of een vraag beantwoord. Hierdoor kunnen sommige taken van de overheid automatisch of sneller worden uitgevoerd. Ambtenaren kunnen dit niet allemaal zelf doen. Dan zouden er namelijk veel meer ambtenaren nodig zijn. Bovendien zou het dan veel langer duren om al die beslissingen te nemen. Daarom zou de overheid haar werk niet goed kunnen doen zonder algoritmes.

Er zitten ook risico's aan het gebruik van algoritmes. Als algoritmes niet goed werken, kunnen groepen mensen worden gediscrimineerd. Ook maken burgers zich zorgen dat de overheid door algoritmes te veel over hun privéleven te weten komt. Andere zorgen zijn dat de overheid algoritmes gebruikt zonder dat te vertellen. En dat de overheid niet aan mensen kan uitleggen hoe een besluit is genomen. Dat geldt niet alleen voor technisch ingewikkelde algoritmes. Het gaat juist ook om simpele algoritmes. Die kunnen net zo goed grote gevolgen hebben voor burgers.

Daarom doet de Algemene Rekenkamer voor de tweede keer onderzoek naar algoritmes. Ons eerste onderzoek heette 'Aandacht voor algoritmes'. Daarin hebben we onderzocht waarvoor de rijksoverheid algoritmes gebruikt. We hebben ook gekeken wat voor soort algoritmes dat zijn. Hierboven hebben we een paar risico's van algoritmes genoemd. Voor elk algoritme kun je controleren hoe groot die risico's zijn. Wij hebben in ons eerste onderzoek een aanpak bedacht om de risico's te

controleren. We hebben op een rij gezet aan welke voorwaarden algoritmes moeten voldoen. Die voorwaarden bij elkaar noemen we het 'toetsingskader'. Met dat toetsingskader kunnen we bekijken of de overheid algoritmes goed gebruikt (Algemene Rekenkamer, 2021). In dit tweede onderzoek hebben we 9 algoritmes onderzocht. We hebben gekeken of ze goed werken volgens ons toetsingskader.

## 1.1 Conclusies

We hebben in ons onderzoek gezien dat 3 van de 9 algoritmes aan het toetsingskader voldoen. Dit laat zien dat je algoritmes op een eerlijke, verstandige manier kunt gebruiken.

We hebben ook gezien dat 6 van de 9 onderzochte algoritmes niet helemaal voldoen aan de voorwaarden in ons toetsingskader. Er zijn nog veel dingen die beter kunnen. De 3 belangrijkste verbeterpunten bespreken we hieronder.

We hebben gezien dat er soms geen goede afspraken worden gemaakt over wat het algoritme moet kunnen. Of dat er geen afspraken worden gemaakt om te controleren of een algoritme werkt zoals de bedoeling is. Dat is extra belangrijk als de overheid een andere organisatie vraagt om een algoritme te maken of te beheren. Het gevaar is dat de overheid zelf dan niet meer in de gaten kan houden of het algoritme veilig gebruikt wordt.

Een ander verbeterpunt is IT-beheer. Algoritmes gebruiken gegevens van mensen en bedrijven. Organisaties die algoritmes gebruiken moeten goede afspraken maken over wie wel en wie niet met die gegevens mag werken. Wij hebben gezien dat niet alle organisaties zulke afspraken hebben gemaakt. Daardoor kunnen de organisaties niet zeker weten of de gegevens van burgers en bedrijven veilig zijn.

Een derde verbeterpunt is bias. *Bias* betekent dat de uitkomsten van het algoritme voor sommige groepen mensen verkeerd zijn. Doordat er een fout zit in een algoritme of doordat er bij het maken van het algoritme verkeerde informatie in het algoritme is gestopt. In ons onderzoek hebben we gezien dat organisaties niet controleren of dat soort fouten in algoritmes zitten. Daardoor kunnen de organisaties niet zeker weten of de uitkomsten van het algoritme voor alle mensen hetzelfde zijn.

## 1.2 Aanbevelingen

Wij vinden dat de overheid algoritmes op een verstandige manier moet gebruiken. Daarom adviseren we hieronder aan ministers hoe ze dat het beste kunnen doen.

We herhalen 2 aanbevelingen die we in het eerste onderzoek ‘Aandacht voor algoritmes’ hebben gedaan (Algemene Rekenkamer, 2021):

1. Leg, met name bij uitbesteding of inkoop bij een andere partij, afspraken over de inzet van algoritmes vast en richt de continue monitoring op het nakomen van deze afspraken in.
2. Zorg dat algoritmes en benodigde data beschermd worden door goed functionerende IT-beheersmaatregelen.

Daarnaast doen we 2 nieuwe aanbevelingen:

3. Controleer voortdurend – tijdens ontwerp en uitvoering – op het effect van bias door algoritmes en voorkom daarmee dat onwenselijke systematische afwijkingen voor specifieke personen of groepen ontstaan.
4. Besteed bij het toezicht op instellingen op afstand van het Rijk ook expliciet aandacht aan de inzet van algoritmes bij de uitvoering van publieke taken.

# 2. Over dit onderzoek

## 2.1 Waarom dit onderzoek?

Algoritmes worden ingezet om handelingen te automatiseren, een probleem op te lossen of een voorspelling te doen. Een algoritme is 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 ondersteunen vaak de bedrijfsvoerings- en dienstverleningsprocessen van organisaties. Zonder algoritmes is bijvoorbeeld het op tijd verwerken van massale aanvragen van subsidies en toeslagen niet mogelijk. Dankzij algoritmes kunnen organisaties ook gericht mensen en middelen inzetten bij controles of inspecties. Daarnaast kunnen algoritmes besluitvormings-processen transparanter en makkelijker controleerbaar maken. Dat komt doordat de techniek achter een algoritme, zoals de databronnen waar een algoritme gebruik van maakt en welke aspecten van de data benadrukt worden, vastligt in instructies. Dit maakt algoritmische besluitvorming in principe transparanter dan menselijke besluitvorming.

De inzet van algoritmes biedt dan ook kansen voor een doelmatige en transparantere overheid. Maar een onzorgvuldige toepassing van algoritmes brengt ook risico's met zich mee, niet alleen voor burgers en bedrijven, maar ook voor de overheid zelf. Overheden hebben steeds meer gegevens van burgers en maken steeds vaker gebruik van algoritmes. Zo komen burgers steeds meer in aanraking met de gevolgen van het gebruik van data en algoritmes door de overheid (Nationale Ombudsman, 2021). Er zijn echter zorgen over de inzet van algoritmes door de overheid, bijvoor-beeld dat algoritmes kunnen leiden tot discriminatie. Dat blijkt onder meer uit

nieuwsberichten over het gebruik van algoritmes door de overheid. Zoals over voor-ingenomen uitkomsten bij het opsporen van uitkeringsfraude, naar aanleiding van onderzoek door de Rekenkamer Rotterdam (Trouw, 2021 en Rekenkamer Rotterdam, 2021). Of over 'de boodschappenzaak', waarbij algoritmes werden gebruikt om gevallen van fraude op te sporen (Volkskrant, 2021). Zorgen over de inzet van algoritmes zijn ook zichtbaar in de Tweede Kamer: in het Kamerdebat over de toeslagenaffaire werd een motie aangenomen waarin werd opgeroepen te stoppen met het gebruik van discriminerende algoritmes (Tweede Kamer, 2021).

Zowel de kansen als de zorgen zijn aanleiding voor ons om de inzet van algoritmes bij de rijksoverheid te onderzoeken. Dit onderzoek is het tweede onderzoek naar algoritmes van de Algemene Rekenkamer. In ons eerste onderzoek, 'Aandacht voor algoritmes', hebben we een toetsingskader ontwikkeld om de inzet van algoritmes te kunnen beoordelen (Algemene Rekenkamer, 2021). Het toetsingskader is een praktisch instrument dat overheidsorganisaties kunnen gebruiken om te toetsen of algoritmes aan bepaalde kwaliteitscriteria voldoen én of de risico's voldoende in beeld zijn en/of worden beperkt.

In dit tweede onderzoek gaan we voor 9 algoritmes na of ze voldoen aan dit toetsingskader voor algoritmes. We beschrijven bovendien voor 1 van de algoritmes de context waarin het algoritme functioneert. Een algoritme staat namelijk niet op zichzelf maar is altijd onderdeel van een groter beleids- of uitvoeringsproces.

## 2.2 Wat hebben we onderzocht en hoe hebben we het onderzoek uitgevoerd?

We hebben onderzoek gedaan naar de inzet van algoritmes bij de rijksoverheid en daaraan verbonden organisaties. Dit onderzoek bestaat uit 2 delen:

1. In het eerste deel schetsen we de context van 1 specifiek algoritme.
2. In het tweede deel toetsen we de inzet van 9 algoritmes aan de hand van ons toetsingskader algoritmes.

### 2.2.1 Algoritme in context

In dit onderdeel hebben we een van de algoritmes in detail bestudeerd: het risicomodel dat de Rijksdienst voor Ondernemend Nederland (RVO) gebruikt bij de beoordeling van aanvragen voor de Tegemoetkoming Vaste Lasten (TVL). Voor dit algoritme beschrijven we hoe het onderdeel is van het beleidsproces en het werk van ambtenaren, en wat de impact op burgers en bedrijven is. De volgende vragen staan hierbij centraal:

- Hoe maakt het algoritme deel uit van het beleidsproces?
- Wat is de rol van mensen bij het werken met algoritmes?
- Hoe komt besluitvorming over de inzet van het algoritme tot stand?
- Wat is de impact op burgers en bedrijven?

Om antwoord te krijgen op deze vragen, hebben we interviews gehouden met verschillende medewerkers in de organisatie en bij het Ministerie van EZK. Ook hebben we relevante (proces)documenten geanalyseerd.

### 2.2.2 Inzet van algoritmes getoetst

**Welke algoritmes hebben we getoetst?**
In het onderzoek is voortgebouwd op de inventarisatie die wij bij ons eerste onderzoek over algoritmes hebben uitgevoerd (Algemene Rekenkamer, 2021). Deze lijst hebben we aangevuld met een aantal bronnen, waaronder een inventarisatie van algoritmes in publieke dienstverlening door TNO, de ombudsvisie op gebruik van data en algoritmen door de overheid en diverse mediaberichten (Nationale Ombudsman, 2021 en TNO, 2021). Daarnaast hebben we uitvraag gedaan bij onderzoeksteams van de jaarlijkse verantwoordingsonderzoeken van de Algemene Rekenkamer.

Vervolgens hebben we algoritmes geselecteerd op basis van de volgende criteria:

- *Impact op burgers of bedrijven*
  We hebben algoritmes – of processen waar het algoritme deel van uitmaakt – geselecteerd die veel impact hebben op burgers of bedrijven.
- *Risicogericht*
  We hebben algoritmes onderzocht waarvan we denken dat de kans het grootst is dat het algoritme niet op een juiste manier wordt ingezet.
- *Verschillende domeinen*
  We hebben algoritmes uit verschillende domeinen geselecteerd, zoals het sociaal domein en het veiligheidsdomein.
- *In gebruik*
  De geselecteerde algoritmes moesten bovendien in gebruik zijn. Algoritmes die zijn stopgezet of nog in een pilotfase waren, hebben we niet meegenomen in ons onderzoek.
- *Soorten algoritmes*
  Daarnaast hebben we verschillende soorten algoritmes geselecteerd: van technisch eenvoudige algoritmes, zoals beslisbomen en data-uitwisselingssystemen, tot technisch meer complexe algoritmes, zoals beeldherkenningssystemen en ‘zelflerende’ toepassingen.

Voor dit onderzoek hebben we uiteindelijk 9 algoritmes geselecteerd. De algoritmes die wij hebben geselecteerd, staan in Tabel 1.

**Tabel 1.** *Overzicht van geselecteerde algoritmes*

| Min | Organisatie | Status | Omschrijving algoritme |
|---|---|---|---|
| BZK | **Rijksdienst voor Identiteitsgegevens (RvIG)** | Agentschap | Ondersteunt bij de beoordeling van de kwaliteit van foto's voor identiteits-bewijzen |
| EZK | **Rijksdienst voor Ondernemend Nederland (RVO)** | Agentschap | Risicomodel dat gebruikt wordt bij de beoordeling van aanvragen voor de Tegemoetkoming Vaste Lasten (TVL) |
| FIN | **Toeslagen** | Onderdeel ministerie | Ondersteunt bij de beoordeling van aanvragen voor huurtoeslag in het toeslagenverstrekkingensysteem (TVS) |
| IenW | **Centraal Bureau Rijvaar-digheidsbewijzen (CBR)** | rwt/zbo | Ondersteunt bij de beoordeling van de medische rijgeschiktheid van mensen |
| JenV | **Politie** | rwt | Criminaliteits Anticipatie Systeem (CAS) voorspelt waar en wanneer het risico op incidenten hoog is |
| JenV | **Directoraat-generaal (DG) Migratie** | Onderdeel ministerie | Zoekt intelligent in vreemdelingen-persoonsgegevens of iemand al eerder in Nederland is geregistreerd |
| JenV | **Centraal Justitieel Incassobureau (CJIB)** | Agentschap | Koppelt gegevens voor verkeersboetes aan op kenteken geconstateerde verkeers-overtredingen |
| SZW | **Inlichtingenbureau** | rwt | Levert signalen aan gemeenten voor rechtmatigheidscontrole op bijstands-uitkeringen |
| SZW | **Sociale Verzekerings-bank (SVB)** | rwt/zbo | Ondersteunt bij de beoordeling van AOW-aanvragen |

De onderzochte algoritmes zijn in gebruik bij de rijksoverheid zelf en bij organisaties op afstand van het Rijk. Er zijn verschillende typen instellingen op afstand. In dit onderzoek hebben wij onderzoek gedaan bij een aantal zogenoemde rechtspersonen met een wettelijke taak (rwt) en zelfstandige bestuursorganen (zbo). Dit zijn zelfstandige organisaties op afstand van de rijksoverheid die overheidstaken uitvoeren. Een instellingswet bepaalt de taak en bevoegdheden van de organisatie en legt de relatie met de minister vast. De minister heeft hierdoor bij deze organisaties een toezichthoudende taak en moet over het functioneren en presteren van de organisatie informatie kunnen verstrekken aan de Tweede Kamer.

Onze selectie representeert niet alle algoritmes die de rijksoverheid gebruikt. We hebben de algoritmes namelijk risicogericht geselecteerd. Uit de uitkomsten van ons onderzoek zijn dan ook geen algemene conclusies te trekken over processen, organisaties of de gehele rijksoverheid.

**Onderscheid in verschillende soorten algoritmes**

We kunnen de onderzochte algoritmes onderscheiden op basis van de complexiteit van het algoritme en de rol van het algoritme bij het uitvoeren van beleid.

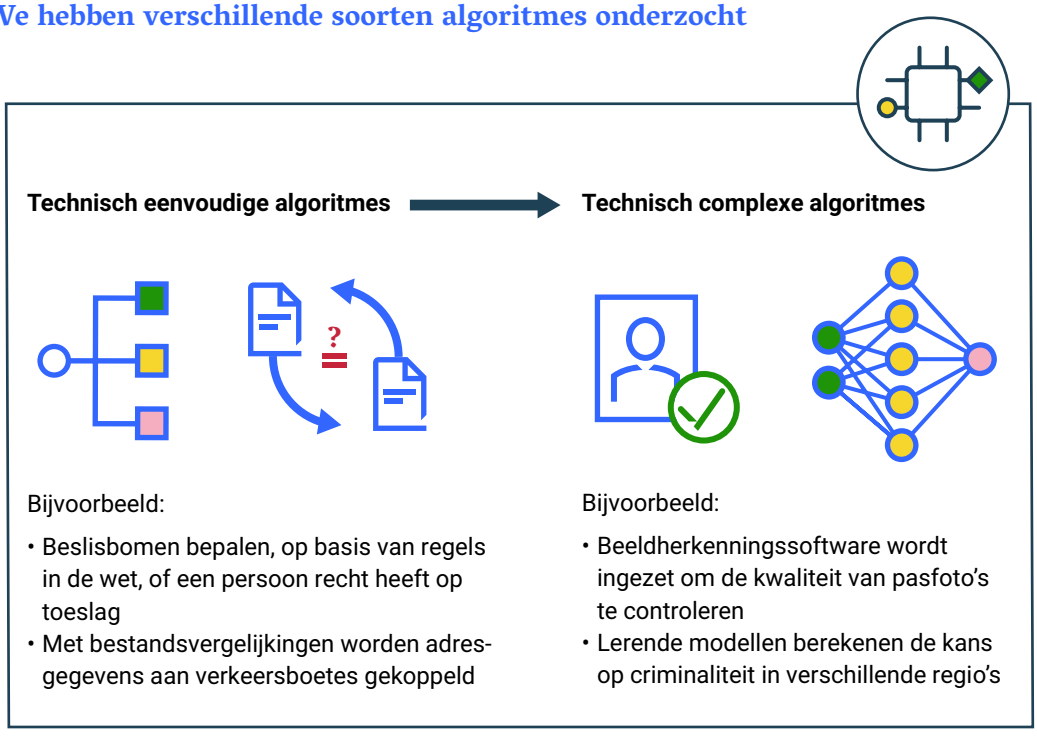
*Complexiteit van het algoritme*

Algoritmes zijn erg verschillend. Algoritmes lopen uiteen van technisch eenvoudig zoals beslisbomen en data-uitwisselingssystemen tot technisch complex zoals beeldherkenningssystemen en lerende algoritmes (Justitie en Veiligheid, 2019).

De onderzochte algoritmes zijn als volgt te verdelen:

- Technisch eenvoudige algoritmes
  - Beslisbomen: Toeslagen, CBR en SVB
  - Data-uitwisselingssystemen: CJIB en Inlichtingenbureau
  - Zoekfunctie: DG Migratie van het Ministerie van JenV
  - Risico-classificatiemodel: RVO
- Technisch complexe algoritmes
  - Beeldherkenningssysteem: RvIG
  - Lerend algoritme: de politie

### We hebben verschillende soorten algoritmes onderzocht



*Rol van het algoritme bij de uitvoering van beleid*

Naast het voorgaande zijn de algoritmes die we hebben onderzocht onder te verdelen in algoritmes die ondersteuning bieden in de uitvoering en algoritmes met (gedeeltelijke) automatische besluitvorming. Een algoritme kan bijvoorbeeld gebruikt worden ter ondersteuning in de uitvoering door ontbrekende gegevens aan te vullen, een voorspelling te doen, of informatie te vergelijken in het kader van risicobeheersing. Bij de tweede categorie algoritmes komen verzoeken van burgers rechtstreeks terecht bij het algoritme. Er is sprake van automatische besluitvorming door een algoritme met directe impact op burgers of bedrijven. Wanneer een aanvraag voldoet aan alle voorwaarden voor toekenning, volgt de aanvraag een geheel automatisch proces waarbij het algoritme besluit. Voldoet de aanvraag niet aan alle voorwaarden, dan volgt een handmatige controle door een ambtenaar.

De onderzochte algoritmes zijn als volgt te verdelen:

- Algoritmes die ondersteuning bieden bij de uitvoering van beleid: Inlichtingenbureau, CJIB, DG Migratie van het Ministerie van JenV, RvIG en de politie
- Algoritmes waarbij sprake is van gedeeltelijke automatische besluitvorming met directe impact op burgers: RVO, CBR, SVB en Toeslagen

Onderstaande tabel laat zien dat geen van de onderzochte algoritmes technisch complex én tegelijkertijd ook besluitvormend is.

**Tabel 2.** *Onderscheid in onderzochte algoritmes*

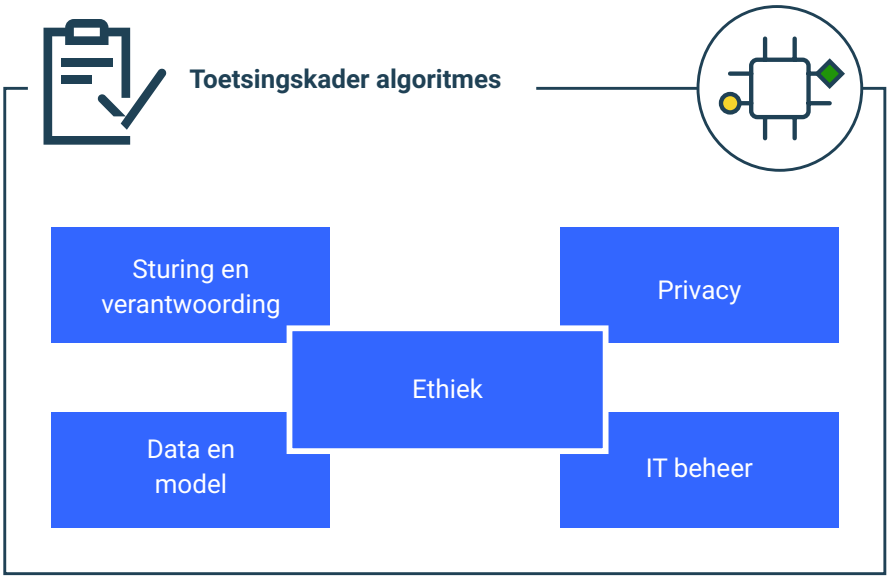
| | Automatische besluitvorming | Ondersteunend |
|---|---|---|
| **Technisch eenvoudig** | • Huurtoeslag (Toeslagen)<br>• Medische rijgeschiktheid (CBR)<br>• AOW-aanvragen (SVB)<br>• TVL-aanvragen (RVO) | • Verkeersboetes (CJIB)<br>• Bijstand (Inlichtingenbureau)<br>• Vreemdelingen (DG Migratie van het Ministerie van JenV) |
| **Technisch complex** | | • Kwaliteit pasfoto's identiteitsbewijzen (RvIG)<br>• Optreden criminaliteit (Politie) |

### Toetsingskader algoritmes

We hebben de inzet van algoritmes beoordeeld aan de hand van het toetsingskader algoritmes (Algemene Rekenkamer, 2021). Het is een praktisch handvat waarmee de rijksoverheid de belangrijkste risico's kan beheersen die zich voordoen bij de inzet van algoritmes. Het toetsingskader bestaat uit de perspectieven sturing en verantwoording, model en data, privacy, IT-beheer en ethiek. Voor elk perspectief zijn de

belangrijkste risico's geformuleerd. Wij koppelen de aspecten en onderzoeksvragen die we willen toetsen aan die risico's. De risico's en onderzoeksvragen uit het toetsingskader staan in bijlage 3.

## We hebben algoritmes onderzocht aan de hand van het toetsingskader algoritmes




Vanuit het perspectief ethiek onderscheiden we 4 ethische principes:

1. respect voor menselijke autonomie;
2. voorkomen van schade;
3. *fairness* (een eerlijk algoritme);
4. verklaarbaarheid en transparantie.

Ethiek is verweven in de 4 overige aspecten uit het toetsingskader. Dat wil zeggen dat de ethische principes zijn gekoppeld aan de risico's van de andere 4 aspecten: sturing en verantwoording, model en data, privacy en IT-beheer.

**Beoordeling van algoritmes**

Door alle vragen uit het toetsingskader te beantwoorden en een score te geven, ontstaat een beeld over de mate waarin risico's beperkt worden bij het gekozen algoritme. Hoe groot de risico's voor een specifiek algoritme zijn, hangt onder meer af van de impact van het algoritme op de burger.

In bijlage 1 staat een uitgebreide toelichting over hoe wij het onderzoek hebben uitgevoerd.

## 2.3 Leeswijzer

Dit onderzoek bestaat uit 2 onderdelen. In hoofdstuk 3 beschrijven we de context van 1 specifiek algoritme en gaan we na hoe dit algoritme wordt ingezet als onderdeel van een beleidsproces. Hoofdstuk 4 bevat onze belangrijkste observaties en aandachtspunten naar aanleiding van het toetsen van de inzet van algoritmes bij de rijksoverheid. Daarna volgt hoofdstuk 5 met onze conclusies en aanbevelingen.

# 3. Een algoritme in zijn context

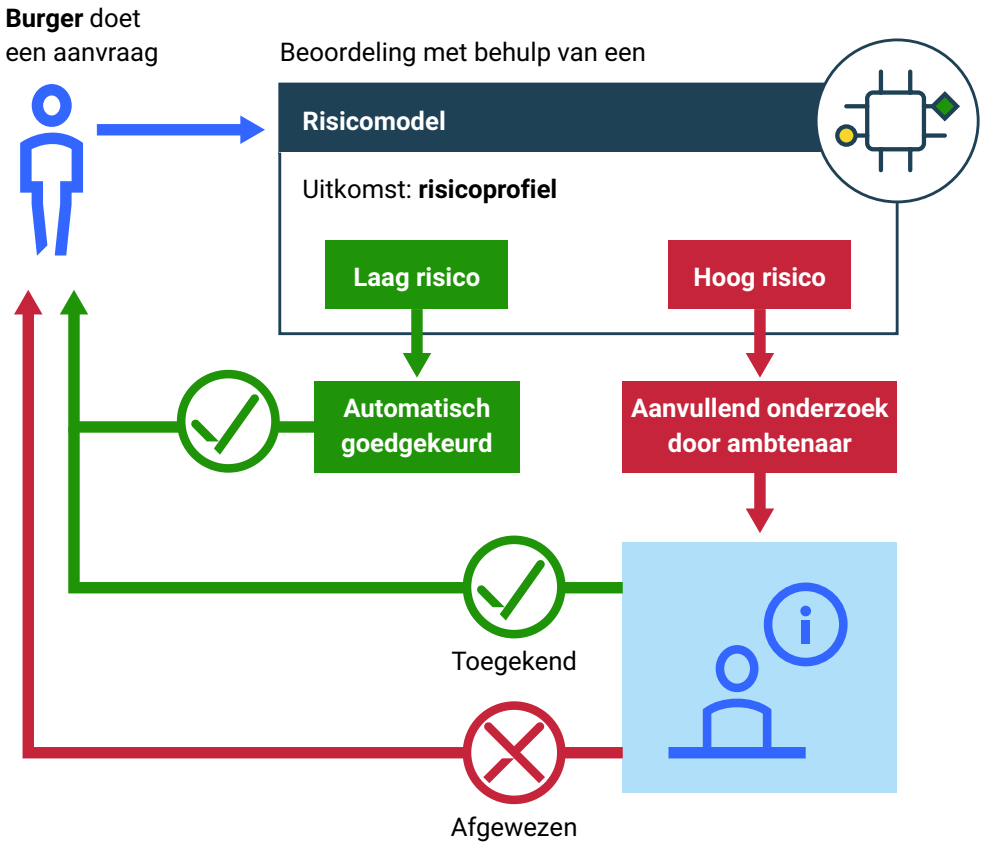
Om de werking van een algoritme te kunnen onderzoeken en duiden is het van belang om de context te kennen waarbinnen een algoritme functioneert. In dit hoofdstuk laten we zien op welke manier een algoritme de RVO helpt bij het uitkeren van de TVL, een financiële regeling om ondernemers tegemoet te komen die omzetverlies lijden door de coronacrisis maatregelen. Zoals we in het vorige hoofdstuk hebben aangegeven, betreft dit een technisch eenvoudig algoritme waarbij sprake is van gedeeltelijke automatische besluitvorming. Voor dit algoritme beschrijven we hoe het onderdeel is van het beleidsproces en het werk van ambtenaren, hoe besluitvorming over de inzet van het algoritme tot stand is gekomen en wat de impact op burgers en bedrijven is.

## 3.1 Werking van het algoritme

De RVO zet een algoritme in als ondersteuning bij de beoordeling van aanvragen van ondernemers. Dit algoritme toetst of een aanvraag voldoet aan de voorwaarden die door de minister zijn gesteld. Dit wordt gedaan met behulp van een risicomodel: als een aanvraag binnenkomt bij de RVO, wordt een inschatting gemaakt of de ondernemer daadwerkelijk recht heeft op de tegemoetkoming. Hierbij vergelijkt de RVO bijvoorbeeld de opgegeven informatie van de aanvrager met andere bij de overheid bekende gegevens, zoals aangiftes bij de Belastingdienst. Een aanvraag wordt automatisch goedgekeurd wanneer de aanvraag door het algoritme als laag risico is aangemerkt, bijvoorbeeld omdat het bedrag waarop de aanvrager aanspraak maakt laag is en er geen aanwijzingen voor misbruik of oneigenlijk gebruik zijn. In dat geval komt er geen ambtenaar meer aan te pas. De ondernemer heeft het geld dan

binnen 5 dagen op zijn rekening staan. Als een aanvraag door het algoritme als hoog risico is aangemerkt, bijvoorbeeld omdat het een hoog bedrag betreft of omdat er aanwijzingen voor misbruik of oneigenlijk gebruik zijn, volgt een handmatige controle. Wanneer bij een eerdere aanvraag misbruik en oneigenlijk gebruik is geconstateerd, zullen toekomstige aanvragen altijd handmatig gecontroleerd worden. Ook wanneer een aanvraag complex is waardoor deze niet automatisch beoordeeld kan worden, volgt een handmatige controle. De aanvraag wordt dan beoordeeld door een ambtenaar. De ambtenaar kan de ondernemer vragen om aanvullende informatie toe te sturen. De ambtenaar besluit vervolgens of de aanvraag wordt toegekend of wordt afgewezen.

### Algoritmes kunnen beleidsprocessen ondersteunen




## 3.2 Besluitvorming over de inzet van een algoritme

Uitvoeringsorganisaties, zoals de RVO, de Sociale Verzekeringsbank (SVB) of de Belastingdienst, voeren overheidstaken uit op basis van wetten die door regering en parlement gemaakt worden. Zij zetten hiervoor regelmatig algoritmes in. Bij besluitvorming over de inzet van een algoritme, is het wenselijk dat zowel het ministerie als de uitvoeringsorganisatie vanaf het begin betrokken is.

Uitvoeringsorganisaties kunnen op die manier adviseren over de uitvoerbaarheid van beleid. En zij kunnen zo samen afspraken maken over het doel van het algoritme, de randvoorwaarden voor de uitvoerbaarheid, of de acceptatie van risico's.

Bij de invoering van de TVL hebben het Ministerie van EZK en de RVO samengewerkt over de opzet van de regeling en hoe een balans kan worden gevonden tussen een snelle uitkering van subsidies, een kleine kans op misbruik en oneigenlijk gebruik van overheidsgelden en praktische uitvoerbaarheid. Tussentijdse bijstellingen van het algoritme worden door de RVO voorgelegd aan het ministerie.

## 3.3 Beperkte rol voor ambtenaren

We hebben gezien dat het algoritme een aanvraag niet automatisch – zonder menselijke tussenkomst – afwijst. Bij afwijzing komt er altijd een mens aan te pas. De vraag is: wat betekent dit in de praktijk? Hoe groot is de rol van ambtenaren?

In het geval van TVL is een ambtenaar betrokken vanaf het moment dat het algoritme een aanvraag als hoog risico aanmerkt. Bijvoorbeeld omdat het een hoog bedrag betreft, de aanvraag incompleet is, of omdat er aanwijzingen zijn voor misbruik of oneigenlijk gebruik. De aanvraag wordt dan klaargezet voor een menselijke beoordeling. Het algoritme geeft een advies mee aan de ambtenaar waar deze op moet letten, zoals gegevens die incompleet of tegenstrijdig zijn. Dit kan nuttig zijn: het advies helpt de ambtenaar om zich snel een beeld te vormen van de situatie. De ambtenaar bekijkt vervolgens de gehele aanvraag. De ambtenaar kan aanvragen vervolgens goedkeuren of afwijzen, eventueel na een nadere uitvraag voor informatie.

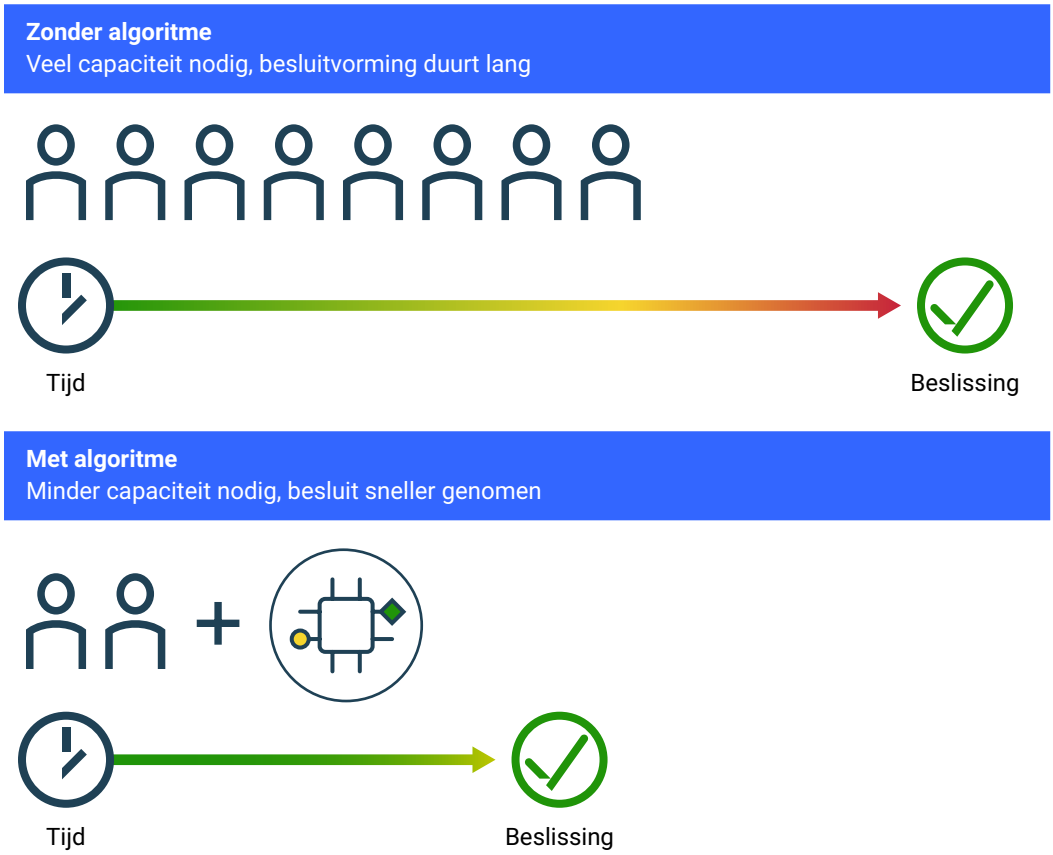
## 3.4 Betekenis van het algoritme voor burgers en bedrijven

Wat betekent het voor ondernemers dat een algoritme wordt ingezet?
De inzet van het algoritme bij TVL-aanvragen zorgt ervoor dat aanvragen snel en doelmatig afgehandeld kunnen worden. Het grootste deel van de ondernemers heeft het geld snel op de rekening staan.

Wanneer een aanvraag wordt geselecteerd voor handmatige controle, moet een ambtenaar de aanvraag beoordelen. In dat geval duurt het langer voordat er een beslissing wordt genomen over de tegemoetkoming, met als gevolg dat het geld later op de rekening van de ondernemer staat.

Daarnaast is het zo dat wanneer bij een eerdere aanvraag misbruik en oneigenlijk gebruik is geconstateerd, toekomstige aanvragen altijd handmatig gecontroleerd zullen worden.

### Inzet van algoritmes kan tijd en capaciteit besparen



# 4. De inzet van 9 algoritmes getoetst

We hebben 9 algoritmes getoetst aan de hand van het toetsingskader algoritmes. Het toetsingskader bestaat uit de thema's sturing en verantwoording, model en data, privacy en IT-beheer. De risico's en onderzoeksvragen uit het toetsingskader staan in bijlage 3. Door alle vragen uit het toetsingskader te beantwoorden en een score te geven, hebben we inzichtelijk gemaakt in hoeverre risico's beperkt worden bij het gekozen algoritme. Hoe groot de risico's voor een specifiek algoritme zijn, hangt onder meer af van de impact van het algoritme op de burger. In bijlage 1 hebben we uitgebreider toegelicht hoe we de algoritmes hebben beoordeeld.

In dit hoofdstuk beschrijven we wat we gezien hebben bij het toetsen van de 9 algoritmes. In onderstaande figuur hebben we voor de 9 onderzochte algoritmes de belangrijkste bevindingen samengevat. Hierin hebben we per thema voor een aantal belangrijke elementen weergegeven hoe hoog het resterende risico is. Onderaan de figuur is weergegeven of de algoritmes voldoen aan het toetsingskader. Een algoritme voldoet aan het toetsingskader indien voor alle belangrijke elementen maatregelen zijn getroffen om de risico's voor het algoritme te verkleinen. Een algoritme voldoet niet helemaal aan het toetsingskader indien op een of meer van de belangrijke elementen het resterende risico hoog is.

Verderop in dit hoofdstuk lichten we onze bevindingen per thema verder toe ($4.3 t/m $4.7).

## Van de 9 onderzochte algoritmes voldoen er 6 niet aan het toetsingskader

## 4.1 3 van de 9 onderzochte algoritmes voldoen aan het toetsingskader

We constateren dat 3 van de onderzochte algoritmes aan het toetsingskader voldoen. Dat betekent dat de organisaties maatregelen hebben getroffen om de risico's uit het toetsingskader voor het algoritme te verkleinen. Dit laat zien dat een verantwoorde inzet van algoritmes wel degelijk mogelijk is.

Deze algoritmes zijn in gebruik bij CBR, CJIB en het Inlichtingenbureau. Het gaat om technisch eenvoudige algoritmes. De onderzochte algoritmes bij het CJIB en het Inlichtingenbureau zijn data-uitwisselingssystemen die ondersteuning bieden in een proces. Het algoritme dat in gebruik is bij het CBR betreft een beslisboom, waarbij sprake is van gedeeltelijke automatische besluitvorming met directe impact op burgers.

Het CJIB gebruikt bijvoorbeeld een algoritme om ervoor te zorgen dat verkeersboetes bij de juiste personen terecht komen. Het algoritme koppelt NAW-gegevens (naam, adres en woonplaats) aan op kenteken geconstateerde verkeersovertredingen. Hiervoor wordt gebruik gemaakt van gegevens van de Rijksdienst voor het wegverkeer (RDW). In ons onderzoek hebben we gezien dat het CJIB afspraken heeft gemaakt over de kwaliteit van de dienstverlening van RDW. Deze afspraken zijn vastgelegd in een Service Level Agreement (SLA). Ook hebben we gezien dat periodiek wordt gemonitord op beschikbaarheid, prestaties en verstoringen. Hierdoor kunnen verkeersboetes op een efficiënte manier naar de juiste personen worden gestuurd.

## 4.2 6 van de 9 onderzochte algoritmes voldoen niet aan het toetsingskader

We constateren dat 6 van de onderzochte algoritmes niet geheel voldoen aan het toetsingskader. Deze zijn in gebruik bij de RVO, Toeslagen, de politie, DG Migratie van het Ministerie van JenV, SVB en RvIG. Bij deze algoritmes is het resterende risico op een of meer van de belangrijke elementen uit het toetsingskader hoog.

Bij 3 organisaties gaat het vooral om het IT-beheer (RVO, Toeslagen en SVB). Deze organisaties moeten nog een aantal stappen zetten zodat ook de effectiviteit van de IT-beheersmaatregelen aantoonbaar voldoende is voor de algoritmes (zie ook $4.6). Zij hebben bijvoorbeeld onvoldoende inzichtelijk of alleen de benodigde medewerkers toegang hebben tot de data en het algoritme, of rechten hebben om wijzigingen aan het algoritme aan te brengen. Hierdoor is de kans groter dat ook andere personen

toegang hebben tot het algoritme en gebruikte gegevens. Ongeautoriseerde toegang tot de systemen kan bijvoorbeeld leiden tot wijziging, beschadiging en/of verlies van data. Met mogelijk grote gevolgen voor burgers en bedrijven.

Bij de andere 3 organisaties (Politie, DG Migratie van het Ministerie van JenV en RvIG) gaat het om het op meerdere aspecten onvoldoende beheersen van de risico's. We zien onder meer de volgende resterende risico's: onvoldoende afspraken en monitoring bij uitbesteding, geen controles op bias en IT-beheer schiet tekort.
De belangrijkste risico's lichten we in dit hoofdstuk ($4.3 t/m $4.6) verder toe.

### Het niet inzetten van algoritmes brengt ook nadelen met zich mee

Een aantal van de algoritmes die wij aanvankelijk hadden geselecteerd voor ons onderzoek, waren bij de start ervan niet (meer) in gebruik. Het gaat om het risicoclassificatiemodel bij Toeslagen en de risicoscan persoonsgebonden budget (PGB) bij de SVB.

#### Risicoclassificatiemodel bij Toeslagen

Het risicoclassificatiemodel werd vanaf april 2013 binnen Toeslagen gebruikt om te selecteren welke toeslagaanvragen voor een handmatige behandeling in aanmerking kwamen. In juli 2020 is het gebruik van het model stilgelegd, omdat het model niet voldeed aan de eisen die de Algemene verordening gegevensbescherming (AVG) daaraan stelt (Financiën, 2020). De risico's op het gebied van privacy en de bijbehorende maatregelen om de negatieve effecten te verminderen of weg te nemen, waren onvoldoende beschreven in een *Data Protection Impact Assessment* (DPIA) (Financiën, 2021). De Autoriteit Persoonsgegevens heeft geconstateerd dat er met het gebruik van nationaliteit in het algoritme sprake was van een overtreding en heeft dit als discriminerend aangemerkt (Autoriteit Persoonsgegevens, 2020).

Het stilleggen van dit model brengt echter ook nadelen met zich mee voor de uitvoering van rechtmatigheidscontroles. Toen het risicomodel nog in gebruik was, werden de aanvragen met het hoogste risico op fouten geselecteerd voor handmatige behandeling. Daarbij werd het aantal te controleren aanvragen gebaseerd op de beschikbare behandelcapaciteit. Met andere woorden: als er weinig capaciteit beschikbaar was, bood Toeslagen alleen de beschikkingen met het allerhoogste risico op fouten ter beoordeling aan behandelaren aan (Financiën, 2021). Zonder algoritme zijn meer mensen nodig om aanvragen te controleren.

**PGB-risicoscan bij de Sociale Verzekeringsbank**

In 2019 heeft de SVB een pilot uitgevoerd om oneigenlijk gebruik en fraude van het persoonsgebonden budget (PGB) te beperken: de pilot PGB-risicoscan. De PGB-risicoscan gaf gemeenten inzicht in mogelijke risico's op misbruik en oneigenlijk gebruik van het PGB. Hoewel de uitkomsten van deze pilot veelbelovend waren, heeft de minister van VWS besloten de pilot PGB-risicoscan stil te leggen. Voor landelijke uitrol van de PGB-risicoscan – en het op structurele basis uitvoeren van risicoanalyses – is namelijk aanpassing van de wet nodig (VWS, 2020). De minister van VWS verwachtte uiterlijk eind 2020 uitsluitsel te kunnen geven over het wel of niet starten van een wetgevingstraject voor een wettelijke grondslag om de PGB-risicoscan landelijk uit te rollen (VWS, 2020). Hier is begin 2022 echter nog geen uitsluitsel over gegeven.

Het niet in gebruik kunnen nemen van de PGB-risicoscan heeft consequenties voor de uitvoering. Het leidt ertoe dat verstrekkers van PGB's momenteel informatie, signalering en inzicht missen om adequaat te kunnen handelen wanneer er sprake is van misbruik van de PGB-regeling. De huidige manier van werken vergt veel handmatig werk en dat kost capaciteit.

## 4.3 Sturing en verantwoording

Met sturing en verantwoording bedoelen we het schriftelijk vastleggen van de rollen, verantwoordelijkheden en deskundigheid, risico-afwegingen bij het gebruik van het algoritme en afspraken met externe partijen over bijvoorbeeld aansprakelijkheid.

**Doelstelling, risicoafweging en monitoring**

In veel gevallen hebben organisaties een duidelijk doel voor het algoritme vastgesteld. Minder aandacht is er voor het met enige regelmaat opnieuw vaststellen van de risico's die het gebruik van het algoritme met zich meebrengt. Om een algoritme verantwoord in te kunnen zetten, moet een afweging worden gemaakt van de voordelen en de risico's van de inzet van het algoritme. Die afweging kan namelijk in de tijd veranderen. Ook is meer aandacht nodig voor periodieke metingen of het algoritme nog voldoet aan vastgestelde doelen of kwaliteitseisen.

***Governance* bij uitbesteding**

Uitbesteding van algoritmes ontslaat ministers of uitvoeringsorganisaties niet van hun verantwoordelijkheid. Zij moeten zicht hebben op de algoritmes die hun organisaties inzetten en op de risico's die het gebruik van algoritmes met zich meebrengt.

Zeker bij uitbesteding of inkoop bij andere partijen is het van belang afspraken over aansprakelijkheid vast te leggen. Bij 2 van de onderzochte organisaties was de ontwikkeling en het beheer van het algoritme uitbesteed. Dit was het geval bij DG Migratie van het Ministerie van JenV en RvIG. Bij deze organisaties zagen we dat vastgelegde beheersmaatregelen voor sturing en verantwoording ontbraken. Bijvoorbeeld bij het door ons onderzochte algoritme voor het beoordelen van de kwaliteit van foto's voor identiteitsbewijzen aan de hand van kenmerken dat in gebruik is bij de RvIG. Zij hebben de ontwikkeling en het beheer van het algoritme uitbesteed aan een externe leverancier. Maar dat heeft ertoe geleid dat het algoritme voor de RvIG een *black box* is geworden, omdat in de overeenkomst met de leverancier geen duidelijke afspraken over het algoritme zijn opgenomen. Met als gevolg dat de RvIG niet kan controleren of het algoritme nog doet waarvoor het bedoeld is.

## 4.4 Model en data

Voor het onderdeel model en data kijken we onder meer naar de ontwikkeling en het onderhoud van het algoritme. Een belangrijk onderdeel hiervan is het uitvoeren van controles om de juiste werking van het algoritme te garanderen.

**Controle op volledigheid van gegevensverwerking**
De volledigheid van gegevensverwerking is een belangrijke voorwaarde voor elk type dataverwerking. Het mag niet zo zijn dat burgers, of andere eenheden, onbedoeld uit de verwerking verdwijnen. Dit kan een onjuiste uitkomst geven. Om dit vast te stellen, moet de invoer van een algoritme vergeleken worden met de uitvoer. We constateren dat deze analyses niet altijd worden gedaan. Vaak wordt bij de verwerking van gegevens in massale processen vertrouwd op foutmeldingen en gaat men ervan uit dat de afwezigheid van foutmeldingen een garantie is voor de juiste werking van het algoritme. Dat is niet altijd het geval.

**Controle op juistheid van gegevens**
In het verlengde hiervan ligt een controle op de juistheid van de gegevens die het model verwerkt. Soms zijn gegevens niet beschikbaar of bestaan onvoldoende waarborgen voor de tijdige levering. Als deze controle niet plaatsvindt, kan de juiste werking van het algoritme niet gegarandeerd worden.

**Controle op bias**
Voor een juiste werking van het algoritme is het van belang om te controleren of er onwenselijke bias voor specifieke personen of groepen is ontstaan. Om dat mogelijk te maken, moet het bestuderen van oorzaken van en omgang met mogelijke bias

worden opgenomen in een regulier proces van risicobeheersing van het algoritme. Het valt op dat de door ons onderzochte organisaties niet standaard beschikken over de expertise die hiervoor nodig is. Ook zien we dat in de meeste gevallen geen controles worden gedaan op (het effect van) bias en onjuiste over- of ondervertegenwoordiging van groepen mensen. Hierdoor kunnen we niet uitsluiten dat bij sommige algoritmes een onwenselijke systematische afwijking voor specifieke personen of groepen is ontstaan (zie ook $4.7).

**Bias**

**Wat is bias?**

Bias betekent: onwenselijke systematische afwijkingen van de uitkomsten van het algoritme voor de gehele groep of juist voor specifieke personen of deelgroepen.

**Hoe ontstaat bias?**

In het toetsingskader onderscheiden we bias in het gebruikte model of in de gebruikte data. Bias door het model kan voorkomen wanneer bijvoorbeeld gebruik wordt gemaakt van etniciteit of van andere kenmerken die iets kunnen zeggen over etniciteit (zoals laaggeletterdheid of moskeebezoek). Een voor-beeld van bias door de data is een algoritme dat gebruik maakt van historische gegevens waarbij sprake is geweest van een specifiek beleid op specifieke groepen. Stel dat in het verleden samenwoonfraude intensiever is aangepakt en dat met deze gegevens een algoritme wordt ontworpen voor fraudedetectie. Dan zal het algoritme samenwoonfraude beter voorspellen, omdat deze vorm van fraude vaker voorkomt in de data. En als samenwoonfraude vooral door vrouwen wordt gepleegd dan is sprake van bias naar vrouwen toe. Deze vorm van bias leidt dan tot een intensievere controle van vrouwen, wat kan leiden tot meer geconstateerde overtredingen bij vrouwen. En dat is een vorm van discriminatie.

**Kan bias voorkomen worden?**

In technische zin is bias vaak niet volledig te voorkomen. Het is echter wel mogelijk om bias vast te stellen, door de uitkomsten van het algoritme te analyseren. Het gebruik van een algoritme biedt ook de mogelijkheid om te corrigeren voor bias. Dat kan door controles in te bouwen in het algoritme of de uitkomsten te controleren op onwenselijke systematische afwijkingen.

**Evaluatie van het algoritme**

Bij de ontwikkeling van algoritmes is het belangrijk dat de kwaliteit van het model geëvalueerd wordt door voorspellingen van het algoritme te toetsen, bijvoorbeeld aan eerdere uitkomsten. Uit ons onderzoek blijkt dat de evaluatie

bij een aantal algoritmes niet gebeurt, terwijl die mogelijkheid er wel is. Soms wordt een dergelijke analyse wel uitgevoerd maar ontbreekt een adequate vastlegging. Bijvoorbeeld bij de toekenning van de TVL. Eerdere ervaringen uit het verstrekkingsproces worden wel in nieuwe versies van het algoritme meegenomen, maar een analyse van verschillen tussen toekenning en aanvraag ontbreekt. En dus blijft de vraag onbeantwoord of deze aanvragen terecht worden afgewezen of toegekend.

## 4.5 Privacy

De algoritmes uit ons onderzoek maken allemaal gebruik van persoonsgegevens. Dit brengt voor de verwerker van dergelijke gegevens verantwoordelijkheden met zich mee. Burgers en bedrijven moeten er immers op kunnen vertrouwen dat de overheid goed met hun gegevens omgaat. In ons onderzoek hebben wij gezien dat de meeste onderzochte organisaties oog hebben voor de privacyrisico's. Er worden bijvoorbeeld verwerkingsregisters opgesteld, waarin wordt aangegeven welke persoonsgegevens worden verzameld en verwerkt.

**DPIA**

Uit ons onderzoek blijkt dat aandacht voor de bescherming van persoonsgegevens standaard onderdeel is geworden van de belangenafweging en besluitvorming van (voorgenomen) beleid en regelgeving. Overheidsorganisaties zijn op grond van de AVG in sommige gevallen verplicht om een gegevensbeschermingseffectbeoordeling (ook bekend als DPIA, *Data Protection Impact Assessment*) uit te voeren bij nieuwe gegevensverwerkingen (BZK, 2017). Een DPIA is bijvoorbeeld verplicht als er voor bestaande processen hoge privacyrisico's zijn. Het rijksbrede template voor de DPIA helpt om gemaakte afwegingen vast te leggen. Voor 7 van de 9 onderzochte algoritmes, of de processen waar algoritmes onderdeel van zijn, is een DPIA uitgevoerd. De Rijksdienst voor Identiteitsgegevens heeft geen DPIA opgesteld. Ook de politie heeft geen privacy impact analyse uitgevoerd. Zij missen daarmee een manier om in te zien of alle risico's afgedekt zijn.

**Dataminimalisatie**

Dataminimalisatie houdt in dat je als organisatie niet meer gegevens mag verzamelen dan nodig is om het beoogde doel te bereiken. We hebben gezien dat de meeste organisaties maatregelen hebben getroffen om het niet proportioneel gebruiken of verzamelen van gegevens tegen te gaan. Alleen de politie heeft meer gegevens

verzameld dan nodig was voor het beoogde doel. De politie heeft bijvoorbeeld gegevens over nationaliteit verzameld, maar deze gegevens niet gebruikt voor berekeningen.

**Transparantie**

De mate waarin organisaties informatie delen over omgang met privacy en gegevensverwerkingen, wisselt. Een openbaar privacybeleid is vaak aanwezig, maar daarin is meestal geen informatie over specifieke algoritmes opgenomen. Het CBR, het Inlichtingenbureau en SVB hebben wel een openbaar privacybeleid dat ingaat op de manier waarop gegevens verwerkt worden bij specifieke algoritmes. Op de website van het Inlichtingenbureau is bijvoorbeeld een pagina opgenomen met het algemene privacybeleid (https://www.inlichtingenbureau.nl/Privacy-en-Veiligheid/Privacy-en-burgers). Informatie over de gebruikte algoritmes staan in verschillende verwerkingsregisters. Hierin is bijvoorbeeld informatie opgenomen over het doel van de verwerking, de gebruikte bronnen en de bewaartermijnen van de gegevens. Met deze informatie kunnen betrokkenen en andere geïnteresseerden inzien hoe persoonsgegevens worden gebruikt en wat hun rechten zijn. De RVO en Toeslagen hebben een openbaar algemeen beleid en een specifiek op algoritmes gespitst privacybeleid ingebed in de aanvraagprocedure.

## 4.6 IT-beheer

Bij een verantwoorde inzet van algoritmes is een belangrijke randvoorwaarde dat de gebruikte data en het algoritme zelf worden beschermd. Ongeautoriseerde toegang tot de systemen kan bijvoorbeeld leiden tot wijziging, beschadiging en/of verlies van data. Met mogelijk grote gevolgen voor burgers en bedrijven.

**IT-beheer: de basis op orde**

Een goede inrichting van het IT-beheer is – ook bij de inzet van algoritmes – cruciaal voor het bewaken van de betrouwbaarheid, vertrouwelijkheid en beschikbaarheid van informatiesystemen. Dit houdt onder meer in dat alleen bevoegden toegang hebben tot de systemen, dat medewerkers geen ruimere rechten hebben dan nodig is en dat wijzigingen worden getest voor ingebruikname.

**Wat zijn generieke IT-beheersmaatregelen?**

Generieke IT-beheersmaatregelen (GITC) zijn basisbeheersmaatregelen die organisaties treffen om IT-systemen te beveiligen en te beheersen. In het toetsingskader algoritmes is aandacht voor in ieder geval de volgende traditionele IT-beheerprocessen: toegangsbeheer (wachtwoordbeheer,

gebruikersbeheer en beveiliging van componenten), wijzigingenbeheer en *back-up en recovery*. Deze beheersmaatregelen zijn al jaren onderdeel van het jaarlijkse verantwoordingsonderzoek van de Algemene Rekenkamer.

**IT-beheersmaatregelen bij algoritmes: een aantal voorbeelden**

- Wanneer algoritmes worden gebruikt voor beslissingen die gevolgen hebben voor burgers (bijvoorbeeld bij de beoordeling van AOW-aanvragen), moeten organisaties maatregelen treffen zodat alleen een beperkt aantal medewerkers de code van het algoritme (en daarmee mogelijk de wijze van besluiten nemen) kan veranderen.
- Wijzigingen moeten via een vast proces worden doorgevoerd dat voor de gehele organisatie geldt, zodat een belangrijke verandering in het algoritme bijvoorbeeld niet zomaar kan worden doorgevoerd. Als blijkt dat een grote verandering bijvoorbeeld onterecht een nadelig effect heeft op burgers, moet dit ook kunnen worden teruggedraaid.
- Juist doordat de meeste algoritmes die we hebben onderzocht veel impact kunnen hebben op burgers, is het belangrijk dat alles rondom en in de code van het algoritme wordt vastgelegd. Op die manier kan altijd worden herleid wie welke werkzaamheden heeft uitgevoerd rondom het algoritme. Zo kan worden achterhaald wie er eventueel een fout heeft gemaakt en of iemand misbruik heeft gemaakt van de toegang tot het algoritme. Zo kan de organisatie en de medewerker dit herstellen of hiervan leren.

**Hoe kan een organisatie laten zien dat dat er voldoende zicht is op de risico´s van de gebruikte algoritmes?**

We willen begrijpen wat de algoritmes precies doen, maar ook of de risico's van de algoritmes goed worden onderkend en beheerst. Dat betekent dat het belangrijk is dat organisaties kunnen aantonen dat er maatregelen zijn ingericht om IT-risico's te verkleinen. Of dat organisaties heel bewust besluiten om de risico's die samenhangen met de algoritmes, te accepteren. Laten zien dat IT-beheersmaatregelen ook gelden voor algoritmes, of de omgeving waarin algoritmes zijn ondergebracht, geeft hier invulling aan. IT-audits kunnen daarbij helpen.

**IT-beheer bij algoritmes schiet tekort**

Onze toetsing van de algoritmes laat zien dat dit basis-IT-beheer bij 6 van de onderzochte algoritmes op veel vlakken tekort schiet. We signaleren dat 6 van de onderzochte organisaties geen inzicht hebben of alleen de benodigde medewerkers toegang hebben tot de data en het algoritme, of rechten hebben om wijzigingen

aan het algoritme aan te brengen. Deze problemen met IT-beheer zijn niet uniek voor algoritmes. We zien al jaren problemen op het gebied van IT-beheer bij de rijksoverheid (Algemene Rekenkamer, 2020). Dat beeld wordt hier bevestigd.

We zien ook organisaties die de risico's die samenhangen met toegangsbeveiliging, wijzigingenbeheer en *back-up en recovery* voor het algoritme wel goed beheersen. Dit was het geval bij het CBR, het CJIB en het Inlichtingenbureau.

**Uitbesteding IT-beheer**
Als de ontwikkeling of het beheer van een algoritme is uitbesteed aan een externe partij, zijn ministers of uitvoeringsorganisaties nog steeds verantwoordelijk voor de juiste werking van het algoritme. Dit was het geval bij de Rijksdienst voor Identiteitsgegevens en DG Migratie van het Ministerie van JenV. In ons onderzoek stellen wij vast dat de door ons onderzochte organisaties in dat geval geen inzicht hebben of de risico´s met betrekking tot de algoritmes worden beheerst. Organisaties hebben bijvoorbeeld geen informatie aangeleverd over de IT-beheersmaatregelen of konden onvoldoende aantonen dat de uitbestede IT-beheersmaatregelen werken.

## 4.7 Ethiek

Ethiek is verweven in de 4 verschillende aspecten die we hiervoor hebben beschreven: sturing en verantwoording, model en data, privacy, en IT- beheer. Vanuit het perspectief ethiek onderscheiden we 4 onderwerpen:
1. respect voor menselijke autonomie;
2. voorkomen van schade;
3. *fairness* (een eerlijk algoritme);
4. verklaarbaarheid en transparantie.

**Respect voor menselijke autonomie**
Bij 4 van de onderzochte algoritmes komen verzoeken van burgers of bedrijven rechtstreeks terecht bij het algoritme. Dit is het geval bij de RVO, CBR, SVB en Toeslagen. Er is sprake van automatische besluitvorming door een algoritme met directe impact op burgers of bedrijven. Wanneer een aanvraag voldoet aan alle voorwaarden voor toekenning, volgt de aanvraag een geheel automatisch proces waarbij het algoritme besluit. Voldoet de aanvraag niet aan alle voorwaarden, dan volgt een handmatige controle door een ambtenaar.

Wij hebben gemerkt dat bij gebruik van de besluitvormende algoritmes die wij hebben onderzocht, de aanvrager inzicht krijgt in de logica achter een besluit, bijvoorbeeld

door in een brief het besluit toe te lichten. Burgers krijgen bij de beslissing de mogelijkheid om in bezwaar te gaan.

**Voorkomen van schade**

Bij het voorkomen van schade is het van belang dat de privacy van mensen wordt gewaarborgd en dat goed wordt omgegaan met persoonsgegevens. We hebben gezien dat organisaties veel aandacht hebben voor de bescherming van persoonsgegevens (zie $4.5). Maar bij het voorkomen van schade is het ook van belang dat de gebruikte data en het algoritme zelf worden beschermd, oftewel: het basis-IT-beheer moet op orde zijn. De risico's zijn groot: ongeautoriseerde toegang tot systemen kan leiden tot wijziging, beschadiging en/of verlies van data. Mogelijk met grote gevolgen voor burgers en bedrijven. Uit ons onderzoek blijkt dat het basis-IT-beheer tekort schiet ($4.6).

**Fairness (een eerlijk algoritme)**

Fairness betekent dat het algoritme rekening houdt met diversiteit in de populatie en niet discrimineert. Het is daarbij belangrijk om te benoemen dat ook mensen kunnen discrimineren. Zo heeft PwC in onderzoek naar de Fraudesignaleringsvoorziening (FSV) voorbeelden aangetroffen in communicatie binnen de Belastingdienst dat het risico op fraude werd gebaseerd op nationaliteit en uiterlijk voorkomen (Financiën, 2022 en PwC, 2021). Uit onderzoek van het College voor de Rechten van de Mens blijkt dat de inzet van algoritmes de kans op discriminatie kan vergroten, maar ook kan verkleinen (College voor de Rechten van de Mens, 2020). Hieronder bespreken we 2 manieren waarop de inzet van een algoritme de kans op discriminatie kan vergroten: bias in het algoritme of bias in de data.

*Bias in het algoritme*

Bias door het model kan voorkomen wanneer bijvoorbeeld gebruik wordt gemaakt van een variabele zoals nationaliteit. Het bekendste voorbeeld is het gebruik van nationaliteit in het risicoclassificatiemodel dat tot juli 2020 in gebruik was bij Toeslagen (Financiën, 2020). De Autoriteit Persoonsgegevens heeft geconstateerd dat er met het gebruik van nationaliteit in het algoritme sprake was van een overtreding en heeft dit als discriminerend aangemerkt (Autoriteit Persoonsgegevens, 2020).

Het is echter niet zo dat variabelen zoals nationaliteit of afgeleiden daarvan per se niet gebruikt mogen worden. In sommige gevallen is deze informatie nodig om te controleren of iemand recht heeft op een toeslag of uitkering. Bij 2 organisaties was opname van dergelijke informatie nodig om te controleren of iemand recht heeft op een toeslag of uitkering. De SVB stelt de hoogte van een AOW-uitkering vast op basis

van het aantal jaar dat iemand in Nederland heeft gewoond of gewerkt. Toeslagen beoordeelt bij de aanvraag van huurtoeslag of de aanvrager in Nederland woont en de Nederlandse nationaliteit heeft of een verblijfsvergunning.

6 van de onderzochte organisaties (CBR, CJIB, het Inlichtingenbureau, DG Migratie van het Ministerie van JenV, de RVO en de politie) hebben in hun algoritmes geen variabelen gebruikt die discriminatie in de hand werken, zoals nationaliteit of afgeleiden daarvan. Bij 1 organisatie hebben we geen inzicht in de gebruikte variabelen. De RvIG heeft het algoritme uitbesteed, maar heeft geen zicht op de variabelen die gebruikt worden bij de controle van pasfoto's. Het algoritme is voor RvIG een black box geworden. Daarmee bestaat ook het risico op bias of discriminatie, als bijvoorbeeld pasfoto's van mensen met een bepaalde nationaliteit vaker worden afgekeurd.

*Bias in data*
Een onwenselijke systematische afwijking voor specifieke personen of groepen kan ook ontstaan wanneer bijvoorbeeld historische data wordt gebruikt waar bias in is ontstaan (zie $4.4). Bij de door ons onderzochte organisaties heeft de politie bijvoorbeeld gebruik gemaakt van historische data om aan de hand van een kansberekening de te verwachten criminaliteit in kaart te brengen. Wanneer bias in deze gebruikte historische data is ontstaan, bijvoorbeeld doordat in het verleden bepaalde wijken intensiever zijn gecontroleerd, is de kans groot dat in de voorspellingen onwenselijke systematische afwijkingen ontstaan.

Dit risico komt ook naar voren uit onderzoek dat is uitgevoerd bij gemeenten in opdracht van het College voor de Rechten van de Mens. Alle onderzochte gemeenten benoemden daarin als risico dat er altijd met data uit het verleden wordt gewerkt en dat in de dataset ook een bias kan zitten (Hooghiemstra & Partners, 2021).

Voor een goed functionerend algoritme is het van belang om te controleren of er onwenselijke bias voor specifieke personen of groepen is ontstaan. We kunnen niet uitsluiten dat bij sommige algoritmes toch een onwenselijke systematische afwijking (bias) voor specifieke personen of groepen is ontstaan. We hebben immers gezien dat vaak geen controles worden uitgevoerd om het effect van bias vast te stellen (zie $4.4). Terwijl dit een mooi hulpmiddel zou zijn om het risico op ongewenste bias te ondervangen.

**Verklaarbaarheid en transparantie**
Er zijn 2 soorten transparantie als het gaat om algoritmes: technische transparantie en procedurele transparantie. Technische transparantie houdt in dat eigenaren van

een algoritme de werking ervan moeten kunnen uitleggen. Procedurele transparantie houdt in dat eigenaren van een algoritme verantwoording moeten afleggen over de gevolgde procedure bij de totstandkoming en de uitkomsten van het algoritme. Om te bepalen welke mate van transparantie nodig is, moet ook rekening worden gehouden met de doelgroep. Uit onderzoek van kennisinstituut PON & Telos, in opdracht van het consortium 'Publieke controle op algoritmes', blijkt dat burgers relatief weinig behoefte hebben aan informatie over de technische details. Zij willen vooral geïnformeerd worden over privacy, menselijke controle op het algoritme en de reden waarom het algoritme wordt ingezet (Het PON & Telos, 2021). Voor controleurs is technische transparantie echter wel van belang. Zij moeten namelijk de werking van het algoritme kunnen vaststellen.

In ons onderzoek hebben we gezien dat de technische transparantie vaak geen problemen opleverde. Voor controleurs zoals de Rekenkamer zijn algoritmes vaak geen black box. We hebben voor ons onderzoek inzage gekregen in de gebruikte modellen. De werking van deze modellen was op hoofdlijnen uitlegbaar.

Uit ons onderzoek blijkt dat de procedurele transparantie op sommige vlakken beter kan. Voor burgers en bedrijven is niet altijd inzichtelijk welke data worden gebruikt in welke algoritmes, hoe die algoritmes op hoofdlijnen functioneren en welke impact de uitkomsten daarvan hebben. Organisaties hebben vaak wel een openbaar privacybeleid, maar daarin is niet altijd informatie over specifieke algoritmes opgenomen (zie $4.5). Een algoritmeregister kan een instrument zijn om transparantie te vergroten en burgers beter te informeren. De gemeente Amsterdam heeft een dergelijk algoritmeregister ontwikkeld (https://algoritmeregister.amsterdam.nl/). Het biedt een overzicht van de algoritmes die de gemeente Amsterdam gebruikt bij gemeentelijke dienstverlening.

# 5. Conclusies en aanbevelingen

In dit onderzoek hebben we 9 algoritmes getoetst. We constateren dat 3 van de 9 onderzochte algoritmes aan het toetsingskader voldoen. Dit laat zien dat een verantwoorde inzet van algoritmes mogelijk is. We constateren ook dat 6 van de 9 onderzochte algoritmes niet geheel voldoen aan ons toetsingskader voor algoritmes. Uit ons onderzoek blijkt dat er nog veel verbeterpunten zijn. De belangrijkste hebben betrekking op: afspraken en monitoring bij uitbesteding, IT-beheer en bias. Deze verbeterpunten voorzien we van aanbevelingen.

We herhalen 2 aanbevelingen die we naar aanleiding van het onderzoek 'Aandacht voor algoritmes' in 2021 hebben gedaan (Algemene Rekenkamer, 2021):

1. Leg, met name bij uitbesteding of inkoop bij een andere partij, afspraken over de inzet van algoritmes vast en richt de continue monitoring op het nakomen van deze afspraken in.
2. Zorg dat algoritmes en benodigde data beschermd worden door functionerende IT-beheersmaatregelen.

Daarnaast doen we 2 nieuwe aanbevelingen:

3. Controleer voortdurend – tijdens ontwerp en uitvoering – op het effect van bias door algoritmes en voorkom daarmee dat onwenselijke systematisch afwijkingen voor specifieke personen of groepen ontstaan.
4. Besteed bij het toezicht op instellingen op afstand van het Rijk ook expliciet aandacht aan de inzet van algoritmes bij de uitvoering van publieke taken.

## 5.1 Afspraken en monitoring bij uitbesteding

In navolging van ons eerste onderzoek vragen we aandacht voor het maken van afspraken bij uitbesteding of inkoop van een algoritme bij een externe partij. Wij constateren dat het algoritme een black box wordt wanneer het is uitbesteed, en onduidelijk is welk aspecten van de data worden meegewogen.

**Aanbeveling 1: Leg, met name bij uitbesteding of inkoop bij een andere partij, afspraken over de inzet van algoritmes vast en richt de continue monitoring op het nakomen van deze afspraken in.**
Wij bevelen het kabinet aan om al bij inkoop of uitbesteding van algoritmes afspraken te maken over de doelstellingen en risicoafwegingen en deze vast te leggen en continu te monitoren op het nakomen van deze afspraken. Zo wordt en blijft het inzichtelijk in hoeverre het algoritme voldoet aan de doelstellingen.

## 5.2 IT-beheer

Bij een verantwoorde inzet van algoritmes is een belangrijke randvoorwaarde dat de gebruikte data en het algoritme zelf worden beschermd, oftewel: het basis IT-beheer moet op orde zijn en specifiek op algoritmes gericht. De algoritmes die wij hebben onderzocht, maken gebruik van gevoelige informatie, waaronder persoonsgegevens. Burgers en bedrijven moeten erop kunnen vertrouwen dat deze gegevens veilig zijn. In ons onderzoek constateren we dat het basis IT-beheer echter op veel vlakken tekort schiet. Ook blijkt het IT-beheer te generiek en niet specifiek gericht op het algoritme. Te vaak zien we dat verwezen wordt naar generieke beheersmaatregelen, terwijl algoritmes specifieke bescherming behoeven tegen wijzigingen van het algoritme of manipulatie van de gegevens waar het algoritme gebruik van maakt. We zien al jaren problemen op het gebied van IT-beheer bij de rijksoverheid (Algemene Rekenkamer, 2020). Dat beeld wordt hier bevestigd.

**Aanbeveling 2: Zorg dat algoritmes en benodigde data beschermd worden door goed functionerende IT-beheersmaatregelen.**
Wij bevelen het kabinet aan om ervoor te zorgen dat algoritmes en benodigde data beschermd worden door IT-beheersmaatregelen die specifiek gericht zijn op het algoritme.

## 5.3 Bias

Een goed functionerend algoritme houdt rekening met diversiteit in de populatie en discrimineert niet. Zonder doeltreffende maatregelen kan er een onwenselijke systematische afwijking (bias) voor specifieke groepen personen ontstaan. Voor een juiste werking van het algoritme is het nodig controles uit te voeren, door de uitkomsten van het algoritme te vergelijken tussen verschillende groepen personen zodat systematische afwijkingen in beeld worden gebracht. Ons valt op dat dergelijke controles ontbreken. Terwijl dat een mooi hulpmiddel kan zijn om het risico op bias te ondervangen.

**Aanbeveling 3: Controleer voortdurend – tijdens ontwerp en uitvoering – op het effect van bias door algoritmes en voorkom daarmee dat onwenselijke systematische afwijkingen voor specifieke personen of groepen ontstaan.**
Wij bevelen het kabinet aan om er zorg voor te dragen dat controles worden gedaan op het effect van bias en onjuiste over- of ondervertegenwoordiging van groepen mensen, zodat inzichtelijk wordt of onwenselijke bias voor specifieke personen of groepen is ontstaan. Voor een verantwoorde inzet van algoritmes, zouden dergelijke controles op bias standaard moeten worden opgenomen in een regulier proces van risicobeheersing van het algoritme.

## 5.4 Toezicht op algoritmes bij instellingen op afstand

Algoritmes zijn niet alleen in gebruik bij de rijksoverheid zelf maar ook bij organisaties op afstand van het Rijk. Bovenstaande aanbevelingen gelden niet alleen voor de inzet van algoritmes bij ministeries, maar ook voor de inzet van algoritmes bij instellingen op afstand van het Rijk, de rwt's en zbo's. Het is van belang dat de ministers bij hun toezicht op die instellingen ook expliciet aandacht besteden aan de inzet van algoritmes bij de uitvoering van publieke taken.

**Aanbeveling 4: Besteed bij het toezicht op instellingen op afstand van het Rijk ook expliciet aandacht aan de inzet van algoritmes bij de uitvoering van publieke taken.**
Wij bevelen het kabinet aan om bij het toezicht op instellingen op afstand van het Rijk ook expliciet aandacht te besteden aan de inzet van algoritmes bij de uitvoering van publieke taken. Het toetsingskader kan daar een hulpmiddel bij zijn.

# 6. Reactie en nawoord

Op 11 mei 2022 ontvingen we van de staatssecretaris van Digitalisering en Koninkrijksrelaties een reactie op ons conceptrapport, vanuit haar coördinerende verantwoordelijkheid met betrekking tot digitalisering binnen de rijksoverheid. Hieronder geven we haar reactie samengevat weer ($6.1). De volledige reactie inclusief bijlagen met reacties vanuit de betrokken organisaties staat op www.rekenkamer.nl.
We sluiten dit hoofdstuk af met ons nawoord ($6.2).

## 6.1 Reactie staatssecretaris Digitalisering en Koninkrijksrelaties

In haar reactie dankt de staatssecretaris van Digitalisering en Koninkrijksrelaties (hierna: de staatssecretaris) de Algemene Rekenkamer voor het onderzoek en de meerwaarde die het biedt voor het kwalitatieve handelen van de rijksoverheid. De staatssecretaris geeft aan met deze bevindingen en aanbevelingen verder te werken aan verbeterde dienstverlening en beleidsuitvoering.

De staatssecretaris geeft aan dat er door het gebruik van ons toetsingskader algoritmes een beeld ontstaat van de mate waarin risico's beperkt worden bij de inzet van een algoritme. Het gebruik van het kader helpt in het verder vormgeven van algoritmes en het organiseren van toezicht op het gebruik van algoritmes. Dit wordt dan ook meegenomen in verdere ontwikkelingen die de staatssecretaris hierna beschrijft.

De staatssecretaris geeft aan dat het oordeel van de Algemene Rekenkamer in het onderzoeksrapport stevig is en dat zij om die reden met de departementen aan het

werk gaat om de tekortkomingen aan te pakken. Omdat dit tijd kost, heeft de staatssecretaris de departementen gevraagd om door de daartoe bevoegde experts – zijnde de Chief Information Officer (CIO) en de Functionaris Gegevensbescherming (FG) of Chief Privacy Officer (CPO) – te onderzoeken of het verantwoord is om de zes algoritmes met een midden tot hoog restrisico, te blijven gebruiken totdat de tekortkomingen zijn weggewerkt.

De ontvangen beoordelingen van deze functionarissen geven de staatssecretaris voldoende zekerheid dat de onderkende risico's voor nu voldoende beheerst zijn door genomen maatregelen door de betrokken organisaties voor het verantwoord huidige gebruik van de algoritmes en de daarvoor benodigde data. De reacties van de organisaties zijn als bijlagen toegevoegd aan deze brief (te vinden op www.rekenkamer.nl).

De staatssecretaris beschouwt deze reacties als een eerste stap om enerzijds bewuster om te gaan met de risico's van het gebruik van algoritmes en anderzijds om in gesprek te gaan over de wijze waarop het toetsen van kaders aansluit bij de beheersingsmaatregelen van organisaties.

De staatssecretaris geeft tevens aan dat de organisaties tegelijkertijd met de bevindingen en aanbevelingen uit het rapport aan de slag zijn gegaan, om de restrisico's aan te pakken en daarmee te verkleinen. Daarbij wordt ook geleerd van de organisaties van wie de onderzochte algoritme als 'voldoende' uit het onderzoek kwamen. Een volgende stap wordt dan ook om uitgebreider in te gaan op de bevindingen van de Algemene Rekenkamer. Daarbij zal per organisatie en het daar getoetste algoritme verdere informatie gewisseld worden over het toetsingskader, de gemaakte afwegingen, de risicobeoordeling en bias-controle. Daaruit volgt voor het zomerreces een brief met een aanvullende reactie aan de Tweede Kamer en aan de Algemene Rekenkamer.

## 6.2 Nawoord Algemene Rekenkamer

De staatssecretaris laat met haar ingrijpen zien dat ze niet alleen de resultaten van ons onderzoek maar ook haar coördinerende taak met betrekking tot digitalisering binnen de rijksoverheid serieus neemt.

Wij vinden het positief dat de staatssecretaris in haar reactie aangeeft met de organisaties aan het werk te gaan om de tekortkomingen aan te pakken. De staatssecretaris geeft aan ons en de Kamer nog voor het zomerreces te willen informeren over eventuele vervolgstappen naar aanleiding van de conclusies van ons onderzoek.

Ons valt op dat een aantal onderzochte organisaties in de meegestuurde reacties onze conclusies niet of niet geheel onderschrijft. Daarmee lijken ze af te wijken van de staatssecretaris. Wij wijzen er daarom op dat de diverse onderdelen uit ons toetsingskader niet uit de lucht gegrepen zijn. Ze zijn gebaseerd op bestaande (normen)kaders, richtlijnen en wet- en regelgeving. De generieke IT-beheersmaatregelen uit ons toetsingskader, bijvoorbeeld, zijn gebaseerd op de internationale norm ISO/IEC 27002 en de BIO.

Daarnaast vinden wij de reacties van zowel DG Migratie als de politie zorgelijk. Het lijkt ons goed als de verantwoordelijke vakminister deze organisaties vraagt de door ons signaleerde risico's aan te pakken, omdat deze wel degelijk burgers kunnen raken.

De inzet van algoritmes kan de bedrijfsvoering van de rijksoverheid doelmatiger maken. Daarvan hebben ook burgers en bedrijven profijt. Burgers en bedrijven moeten er echter wel op kunnen vertrouwen dat de inzet van algoritmes door de rijksoverheid op een verantwoorde wijze plaatsvindt. De Algemene Rekenkamer hoopt met dit onderzoek een bijdrage te leveren aan de verantwoorde inzet van algoritmes. Wij zullen de voortgang op alle aanbevelingen volgen en de komende jaren in ons onderzoek aandacht blijven besteden aan de verantwoorde inzet van algoritmes.

# Bijlagen

## Bijlage 1 Hoe wij het onderzoek hebben gedaan

**Onderzoeksvragen**

De onderzoeksvragen voor dit onderzoek waren de volgende:

1. Worden de algoritmes die wij hebben geselecteerd bij de rijksoverheid verantwoord ingezet?
   a. Zijn beheersmaatregelen voldoende effectief om risico's te beheersen?
   b. Voldoen de algoritmes die wij hebben geselecteerd aan de aspecten uit ons toetsingskader algoritmes?
2. Hoe functioneert het algoritme dat wij hebben geselecteerd in de praktijk? Hoe past dit algoritme in het gehele beleidsproces?
   a. Hoe komt besluitvorming over de inzet van dit algoritme tot stand?
   b. Wat doen ambtenaren met de output van dit algoritme? Op basis waarvan worden besluiten genomen?
   c. Wat is de impact op burgers en bedrijven?

**Casusselectie**

In het onderzoek is voortgebouwd op de inventarisatie die wij bij ons eerste onderzoek over algoritmes hebben uitgevoerd. Deze lijst hebben we aangevuld met een aantal bronnen, waaronder:

- inventarisatie media;
- uitvraag bij projectleiders van het verantwoordingsonderzoek van de Algemene Rekenkamer;

- inventarisatie uit *Quickscan AI in publieke dienstverlening II* (TNO, 2021);
- Nationale Ombudsman;
- College voor de Rechten van de Mens.

**Welke algoritmes hebben we getoetst?**

In dit onderzoek hebben we de inzet van 9 algoritmes beoordeeld aan de hand van ons toetsingskader algoritmes. Deze algoritmes zijn geselecteerd op basis van de volgende criteria:

- *Impact op burgers of bedrijven*
  We hebben algoritmes – of processen waar het algoritme deel van uitmaakt – geselecteerd die de veel impact hebben op burgers of bedrijven.
- *Risicogericht*
  We hebben algoritmes onderzocht waarvan we denken dat de kans het grootst is dat het algoritme niet verantwoord wordt ingezet.
- *Verschillende domeinen*
  We hebben algoritmes uit verschillende domeinen geselecteerd, zoals het sociaal domein en het veiligheidsdomein.
- *In gebruik*
  De geselecteerde algoritmes moesten bovendien in gebruik zijn. Algoritmes die zijn stopgezet of nog in een pilotfase waren, hebben we niet meegenomen in ons onderzoek.
- *Soorten algoritmes*
  Daarnaast hebben we verschillende soorten algoritmes geselecteerd. Er zijn namelijk veel verschillende soorten algoritmes: van technisch eenvoudige algoritmes, zoals beslisbomen en data-uitwisselingssystemen, tot technisch meer complexe algoritmes, zoals beeldherkenningssystemen en ‘zelflerende’ toepassingen

**Toetsingskader algoritmes**

De inzet van algoritmes is beoordeeld aan de hand van het toetsingskader algoritmes, ontwikkeld door de Algemene Rekenkamer in het onderzoek ‘Aandacht voor Algoritmes’ (Algemene Rekenkamer, 2021). Het toetsingskader is voor iedereen toegankelijk: www.rekenkamer.nl/algoritmes-toetsingskader.

Het toetsingskader bestaat uit de thema’s sturing en verantwoording, model en data, privacy, en IT beheer. De risico’s en onderzoeksvragen uit het toetsingskader staan in bijlage 3.

**Oordeelsvorming**

De oordeelsvorming over de inzet van algoritmes is als volgt opgebouwd:

1. Wij hebben alle beheersmaatregelen uit het toetsingskader algoritmes beoordeeld op effectiviteit (onderzoeksvraag 1a), aan de hand van aangeleverde documentatie en gesprekken. Een beheersmaatregel kan ‘effectief’, ‘deels effectief’ of ‘niet effectief’ zijn.
2. Wij hebben het restrisico bepaald: laag, midden of hoog. Bij niet effectieve beheersmaatregelen is het restrisico standaard hoog. Dit risico kan naar midden of laag worden teruggebracht aan de hand van de context en/of andere aanvullende maatregelen.
3. Wij hebben het eindoordeel bepaald: de inzet van het algoritme voldoet wel/niet aan het toetsingskader. Dit is een oordeel over alle beheersmaatregelen en risico´s heen.

*Beoordeling van effectiviteit van de beheersmaatregelen*

De effectiviteit van de beheersmaatregelen hebben wij beoordeeld aan de hand van aangeleverde documentatie, gesprekken en waarneming tijdens gesprekken. We hebben onderzochte organisaties gevraagd om per risico uit het toetsingskader algoritmes toe te lichten en te onderbouwen (in de vorm van documentatie) hoe de risico’s zijn beperkt. Deze informatie hebben wij vervolgens beoordeeld en voor afstemming teruggelegd bij de onderzochte organisaties. Op basis van deze reacties en aanvullende documentatie hebben wij de effectiviteit van de beheersmaatregelen opnieuw beoordeeld en het ingevulde toetsingskader definitief gemaakt.
De beoordeling heeft altijd eerst plaatsgevonden door minimaal 2 personen, en daarna voor alle algoritmes in samenspraak met het onderzoeksteam van de Algemene Rekenkamer. Daarbij hebben wij de beoordeling ook gecontroleerd op interne en externe consistentie.

# Bijlage 2 Literatuur


Algemene Rekenkamer (2020). *Staat van de rijksverantwoording 2019*. Den Haag: eigen beheer.

Algemene Rekenkamer (2021). *Aandacht voor algoritmes.* Den Haag: eigen beheer.

Autoriteit Persoonsgegevens (2020). *Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*. Den Haag.

BZK (2017), Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA). Rapportnummer 105172. Den Haag.

College voor de Rechten van de Mens (2020). *Als computers je CV beoordelen, wie beoordeelt dan de computers? Algoritmes en discriminatie bij werving en selectie*. Utrecht.

Europese Commissie (2019). *Ethic guidelines for trustworthy AI*.

Europese Commissie (2020). *Whitepaper on Artificial Intelligence – A European approach to excellence and trust.*

Financiën (2020). Brief van de staatssecretarissen van Financiën. *Nadere informatie over de Fraude Signalering Voorziening (FSV) en het gebruik van FSV binnen de Belastingdienst*. Tweede Kamer, vergaderjaar 2019-2010, 31 066, nr. 681.

Financiën (2021). Brief van de staatssecretaris van Financiën – Toeslagen en Douane. *Openbaarmaking Risicoclassificatiemodel Toeslagen*. Tweede Kamer, vergaderjaar 2021-2022, 31 066, nr. 923.

Financiën (2022). Brief van de staatssecretaris van Financien – Fiscaliteit en Belastingdienst. *Rapporten PwC over FSV – Particulieren en externe gegevensdeling*. Tweede Kamer, vergaderjaar 2021-2022, 31 066, nr. 957.

Het PON & Telos (2021). *Informatiebehoeften van burgers over de inzet van algoritmes door overheden*. Tilburg.

Hooghiemstra & Partners (2021). *Hoe gemeenten besluiten over algoritmen & mensenrechten. Onderzoek voor het College voor de Rechten van de Mens*. Den Haag.

Justitie en Veiligheid (2019). *Bijlage bij Brief over waarborgen tegen risico's van data-analyses door de overheid*. Tweede Kamer, vergaderjaar 2019-2022, 26 643, nr. 641.

Nationale Ombudsman (2021). *Een burger is geen dataset. Ombudsvisie op behoorlijk gebruik van data en algoritmen door de overheid*. Rapportnummer: 2021/021. Den Haag.

PwC (2021). *Onderzoek effecten FSV Particulieren*. Amsterdam.

Rekenkamer Rotterdam (2021). *Gekleurde technologie. Verkenning ethisch gebruik algoritmes.* Rotterdam.

TNO (2021). *Quickscan AI in publieke dienstverlening II*. In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Den Haag.

Trouw (2021, 15 april). *De Rekenkamer waarschuwt Rotterdam: groot risico op discriminatie en profilering door algoritmes*. Geraadpleegd op 28-02-2022 via https://www.trouw.nl/binnenland/de-rekenkamer-waarschuwt-rotterdam-groot-risico-op-discriminatie-en-profilering-door-algoritmes~b58eb5b9/.

Tweede Kamer (2021). *Motie van het lid Klaver c.s. Parlementaire ondervraging kinderopvangtoeslag.* Tweede Kamer, vergaderjaar 2020–2021, 35 510, nr. 16.

De Volkskrant (2021, 23 april). *Staat licht in jacht op uitkeringsfraude burgers volledig door tot verbazing van privacy experts*. Geraadpleegd op 28-02-2022 via https://www.volkskrant.nl/nieuws-achtergrond/staat-licht-in-jacht-op-uitkerings-fraude-burgers-volledig-door-tot-verbazing-van-privacy-experts~b41a35c6/.

VWS (2020). Brief van de minister van Volksgezondheid, Welzijn en Sport. *Persoons-gebonden Budgetten*. Tweede Kamer, vergaderjaar 2019-2020, 25 657, nr. 332.

# Bijlage 3 Toetsingskader algoritmes

Het toetsingskader algoritmes is ontwikkeld in het kader van ons onderzoek *Aandacht voor Algoritmes* (Algemene Rekenkamer, 2021). Het is een praktisch handvat waarmee de rijksoverheid de belangrijkste risico's kan beheersen die zich voordoen bij de inzet van algoritmes. Bij de ontwikkeling van het toetsingskader hebben we gebruikgemaakt van bestaande (normen)kaders, richtlijnen en wet-en regelgeving.

**Algemene vragen**

Voordat het toetsingskader gebruikt wordt, moeten gebruikers eerst een aantal algemene vragen beantwoorden. Deze antwoorden schetsen een algemeen beeld en de context van het algoritme. Deze algemene informatie en context bepalen welke vragen in het toetsingskader relevant zijn voor het algoritme dat wordt getoetst.

1. Wat is de naamgeving van het algoritme of het systeem waar het algoritme deel van uit maakt?
2. In welk werkproces of voor welk product of dienst speelt dit algoritme een rol?
3. Maakt het algoritme gebruik van persoonsgegevens (AVG)?
4. Is er sprake van een lerend algoritme, dat wil zeggen een algoritme dat ontwikkelt en verbetert in de loop van de tijd door gebruik te maken van data en/of ervaringen?
5. Adviseert/ondersteunt het algoritme bij acties/besluitvorming door mensen of handelt het autonoom/automatisch zonder menselijke tussenkomst?
6. Van welke technologie maakt het algoritme gebruik en/of van welke applicatie/software?
7. Welke data(bronnen) gebruikt het algoritme?

**5 perspectieven**

Het toetsingskader kent 5 perspectieven:

1. sturing en verantwoording;
2. model en data;
3. privacy;
4. IT beheer;
5. ethiek.

Voor elk perspectief zijn de belangrijkste risico's geformuleerd. Wij koppelen de aspecten en onderzoeksvragen die we willen toetsen aan die risico's. Door alle vragen te beantwoorden en een score te geven, ontstaat een beeld over de mate waarin risico's beperkt worden bij het gekozen algoritme. Hoe groot de risico's voor een specifiek algoritme zijn, hangt onder meer af van de impact van het algoritme op de burger.

**Ethiek**

De vragen in het toetsingskader zijn mede opgesteld aan de hand van ethische principes (Europese Commissie, 2019; Europese Commissie, 2020). Vanuit het perspectief ethiek onderscheiden we 4 onderwerpen:

- respect voor menselijke autonomie;
- voorkomen van schade;
- *fairness* (een eerlijk algoritme);
- verklaarbaarheid en transparantie

De nummers refereren aan een ethisch principe. De ethische principes zijn gekoppeld aan de risico's van de andere 4 principes: sturing en verantwoording, model en data, privacy en IT beheer.

| Nr. | Ethisch raamwerk | Ethisch principe |
|---|---|---|
| 1.1 | Respect voor menselijke autonomie | De beslissingen die gemaakt zijn door het algoritme zijn te controleren d.m.v. menselijke tussenkomst |
| 2.1 | Voorkomen van schade | Het algoritme is veilig en doet ten alle tijden waar het voor gemaakt is |
| 2.2 | | Privacy is gewaarborgd en data is beschermd |
| 3.1 | Fairness (eerlijke algoritmes) | Het algoritme houdt rekening met diversiteit in de populatie en discrimineert niet |
| 3.2 | | Er is bij de ontwikkeling van het algoritme rekening gehouden met impact op maat-schappij en milieu |
| 4.1 | Verklaarbaarheid en transparantie | Er kan verantwoording worden afgelegd over de gevolgde procedures |
| 4.2 | | De werking van het algoritme is te verklaren en uit te leggen |

### Het toetsingskader algoritmes

Hieronder staan de risico's en onderzoeksvragen uit het toetsingskader algoritmes.

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| 1 | Sturing en verantwoording | | |
| **1.01** | Zonder eenduidigheid over het doel is geen sturing op en verantwoording over het algoritme mogelijk | Is het doel van het algoritme vastgesteld? | 4.2 |
| **1.02** | Zonder actueel beeld van risico's kan er geen goede afweging worden gemaakt of de voordelen van de toepassing van het algoritme opwegen tegen de nadelen | Vindt er op vastgelegde (periodieke) momenten een afweging plaats van de risico's over het gebruik van het algoritme? | 4.1 |
| **1.03** | Zonder voldoende deskundigheid (kwalitatief en kwantitatief) is er een groter risico op fouten | Beschikt de organisatie over voldoende deskundigheid, zowel kwalitatief als kwantitatief? | |
| **1.04** | Een incompleet beeld op de levens-cyclus (life cycle) van het algoritme bemoeilijkt sturing en beheersing | Is het complete lifecycle-management-proces rondom het algoritme gedocumenteerd? | |
| **1.05** | Onduidelijkheid over rollen, taken, verantwoordelijkheden en bevoegd-heden creëert risico's | Zijn de rollen, taken, verantwoordelijk-heden en bevoegdheden in het proces beschreven (inclusief eigenaarschap) en in de praktijk toegepast? | 4.1 |
| **1.06** | Prestatiedoelstellingen en kwaliteits-doelstellingen zijn niet meetbaar of bespreekbaar als er geen aanpak is | Is er een overeengekomen en vastgelegde aanpak voor kwaliteits- en prestatiedoelstellingen voor algoritmes? | 4.2 |
| **1.07** | Afhankelijkheid van externe deskundigen die na het ontwikkelen van het algoritme met de betreffende kennis en ervaring weggaan, waardoor continuïteit en beheersing daarna niet meer gewaarborgd is | Zijn bij uitbesteding van onderdelen of activiteiten met betrekking tot het algoritme afspraken met betrokken externe partijen gemaakt en vastgelegd? | 4.1 |
| **1.08** | Zonder monitoring is er geen beheersing mogelijk | Wordt het algoritme op periodieke basis gemonitord? Je kunt hierbij denken aan monitoring op beschik-baarheid, prestaties/kwaliteit, en of het algoritme voldoet aan actuele wet- en regelgeving | |

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| **2** | **Model en data** | | |
| **2.01** | Algoritme functioneert niet in lijn met geformuleerde doelstellingen | Is het doel van het algoritme duidelijk geformuleerd en is dat geoperationaliseerd in bruikbare aspecten binnen het te gebruiken model en de te gebruiken data? Welke taak of welk onderdeel van de bedrijfsvoering ondersteunt het algoritme? | 4.2 |
| **2.02** | Zonder gedeeld beeld van de doelstellingen is er een groter risico op fouten en/of verschillen in interpretatie | Is er een gedeeld doel van het algoritme en is dat inzichtelijk/uitlegbaar voor eigenaar, ontwikkelaar en gebruiker? | 4.2 |
| **2.03** | Niet of slecht uitlegbare toepassing van algoritmes | Is het algoritme uitlegbaar en heeft er een afweging plaatsgevonden tussen de uitlegbaarheid van het model en de prestatie van het model? | 4.2 |
| **2.04** | Het is niet meer te herleiden waarom welke keuzes zijn gemaakt in ontwerp en implementatie | Zijn de gemaakte overwegingen van het ontwerp en de implementatie vastgelegd? | 4.1, 2.1 |
| **2.05** | Geen continuïteit van het proces/ de uitvoering van werkzaamheden doordat documentatie ontbreekt | Is er documentatie die het ontwerp en de implementatie beschrijft? | 4.1 |
| **2.06** | Er heeft een willekeurige selectie van hyperparameters plaatsgevonden en daarbij zijn onjuiste keuzes gemaakt. Een hyperparameter is een parameter of variabele waarmee kan worden gestuurd op het trainings-/leerproces | Zijn de keuzes voor het gebruik van hyperparameters beargumenteerd en onderbouwd? | |
| **2.07** | Ontbreken van transparantie voor burgers/bedrijven/stakeholders, niet voldoen aan wet- en regelgeving over transparantie | Is het model (code en werking) gepubliceerd en beschikbaar voor belanghebbenden? In hoeverre zijn de gebruikte data of een beschrijving daarvan gepubliceerd en beschikbaar voor belanghebbenden? | |
| **2.08** | Gebruik van geautomatiseerde besluitvorming wanneer dat niet is toegestaan of ontbreken van de mogelijkheid van menselijke tussenkomst | Als er sprake is van geautomatiseerde besluitvorming, wordt daarbij voldaan aan de wet- en regelgeving die daarvoor geldt? | 1.1, 2.1 |
| **2.09** | Te eenzijdige inbreng vergroot kans op fouten en niet voldoen aan doelen en aan wet- en regelgeving | Zijn de verschillende stakeholders/ eindgebruikers van het algoritme betrokken in het ontwikkelproces? | 3.1 |

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| **2.10** | Werking niet volgens vooraf vastgestelde opzet en werking | Welke controles zijn toegepast om de aansluiting te maken tussen de invoer en de uitvoer om zo de juistheid en volledigheid van de verwerking te garanderen? | 2.1 |
| **2.11** | Model is ontwikkeld op basis van regelgeving van jaar t-1, en wordt ingezet in jaar t. De regelgeving (grenswaarden, bedragen) kan ondertussen veranderd zijn of bepaalde bepalingen kunnen niet meer geldig zijn | Wordt het model periodiek geactualiseerd in lijn met actuele wet- en regelgeving? | |
| **2.12** | Onjuiste manier van training/testen kan leiden tot *overfitting* en/of *underfitting* en/of bias (onwenselijke systematische afwijking) | Is de kwaliteit gewaarborgd als het gaat om keuzes die zijn gemaakt bij training- en testdata? | 4.1 |
| **2.13** | Het model creëert onwenselijke systematische afwijking voor specifieke personen, groepen of andere eenheden (bias) | Wordt er gewaarborgd dat er geen bias wordt gecreëerd door keuzes met betrekking tot het model? | 3.1, 3.2 |
| **2.14** | Er zit onwenselijke systematische afwijking (bias) in de data | Bevat de data geen onwenselijke bias? | 3.1, 3.2 |
| **2.15** | Als er niet wordt gescheiden tussen training-, test- en validatiedata, dan is er sprake van overfitting en kan het model niet gebruikt worden voor nieuwe observaties | Zijn training-, test- en validatiedata gescheiden verwerkt? | |
| **2.16** | De data zijn niet representatief | Zijn de gebruikte data representatief voor de toepassing? | 2.1, 3.1, 4.1 |
| **2.17** | Afhankelijkheid van derden met betrekking tot gebruikte data | Heeft de (overheids)organisatie volledige controle en beheersing (eigenaarschap) over de gebruikte data voor het model? | |
| **2.18** | Overtreden van geldende uitgangs-punten/regels met betrekking tot dataminimalisatie en proportionaliteit | Is er sprake van dataminimalisatie? Is gekeken naar proportionaliteit en subsidiariteit? | 2.1 |
| **2.19** | De *performance metrics* komen niet overeen met de doelstellingen van het algoritme | Is de kwaliteit van het model gedocumenteerd? | 4.2 |
| **2.20** | De data waarop het model is gebaseerd, zijn niet beschikbaar voordat de uitkomsten zijn geobserveerd | Is er *target leakage*? Met andere woorden: maken de voorspellingen deel uit van de model features? | |

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| **2.21** | Kwaliteit van de voorspelling is niet op orde | Wordt er gebruikgemaakt van prestatie-indicatoren of performance metrics? | 2.1, 4.2 |
| **2.22** | Soms werkt het model in de praktijk niet (meer) | Wordt de output van het model gemonitord? | 2.1 |
| **2.23** | Het is voor mensen niet duidelijk dat zij met een algoritme te maken hebben, welke consequenties dat heeft of welke beperkingen het algoritme kent. Bij incidenten/fouten kan dit leiden tot schadeclaims achteraf | Vindt er externe communicatie plaats over het model/algoritme, inclusief de beperkingen: wat kan het wel en wat niet? | 4.2 |
| **2.24** | Het risico bestaat dat alle focus en effort aan de voorkant wordt gestoken in het ontwikkelen en in productie brengen van het algoritme, zonder overdracht naar degenen die het algoritme moeten beheren en ook 'de business' vergeten wordt in het onderhoud | Vindt er onderhoud en beheer plaats op het algoritme? | |
| **3** | **Privacy** | | |
| **3.01** | Niet voldoen aan wettelijke verplichting AVG voor bijhouden register | Wordt er een register bijgehouden voor het gebruik van persoonsgegevens? | 2.2 |
| **3.02** | Ontwerp en opzet zijn onvoldoende gericht op bescherming van privacy | Is er sprake van data protection by design? | 2.2 |
| **3.03** | Niet voldoen aan wettelijke verplichting AVG voor uitvoeren DPIA | Is er een DPIA uitgevoerd (indien van toepassing)? | 2.2 |
| **3.04** | Automatische besluitvorming terwijl dat volgens AVG niet is toegestaan | Is er sprake van automatische besluit-vorming en zo ja, is dit toegestaan? | 2.2 |
| **3.05** | Niet voldoen aan wettelijke verplichting AVG/hanteren menselijke maat | Hebben de betrokkenen de mogelijk-heid niet onderworpen te zijn aan geautomatiseerde besluitvorming (indien van toepassing)? | 2.2 |
| **3.06** | Niet proportioneel gebruik/verzameling van persoonsgegevens | Is er sprake van data-minimalisatie? | 2.2 |
| **3.07** | Niet-wettelijk handelen met betrekking tot verwerking van gegevens | Vindt de verwerking van gegevens plaats op grond van een wettelijke taak? | 2.2 |
| **3.08** | Niet voldoen aan doelbinding volgens AVG | Is de verwerking van (bijzondere) persoonsgegevens met het algoritme verenigbaar met het oorspronkelijke doel? | 2.2 |

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| **3.09** | Niet voldoen aan wettelijke verplichting AVG met betrekking tot vastlegging van verantwoordelijkheden | Is vastgesteld wie de verwerkingsverantwoordelijke en verwerker is van de persoonsgegevens van het algoritme en de daarbij gebruikte data? | 2.2 |
| **3.10** | Handelen in strijd met artikel 1 uit de Grondwet (GW)/artikel 14 Europees Verdrag voor de Rechten van de Mens (EVRM) | Is er sprake van discriminatie door gebruikte data en model? | 2.2 |
| **3.11** | Profilering in de zin van AVG, art. 4, sub 4: risico handelen in strijd met AVG | Is er getoetst in hoeverre er sprake is van profilering en in hoeverre dat is toegestaan? | 2.2 |
| **3.12** | Niet voldoen aan wettelijke verplichting AVG met betrekking tot informeren betrokkenen | Is er invulling gegeven aan het proactief of op verzoek informeren van betrokkenen van wie gegevens worden verwerkt/gebruikt (zowel data als algoritme)? | 2.2 |
| **3.13** | Niet voldoen aan wettelijke verplichting AVG en algemene beginselen behoorlijk bestuur (abbb's) met betrekking tot logica en toegankelijkheid | Zijn de logica van het gebruikte algoritme en de gebruikte gegevens voldoende duidelijk voor betrokkenen? | 2.2 |
| **3.14** | Niet voldoen aan wettelijke verplichting AVG met betrekking tot impact op betrokkenen | Zijn de gevolgen van de toepassing van het gebruikte algoritme duidelijk voor betrokkenen? | 2.2 |
| **3.15** | Betrokkenen zijn niet op de hoogte van hun rechten, gebruikte algoritmes en data | Is er een openbaar privacybeleid waarin gebruikte data en algoritmes aan bod komen? | 2.2 |
| **4** | **IT beheer** | | |
| **4.01** | Zonder loginformatie is niet te achterhalen wanneer er aanpassingen zijn gedaan (*audit trail*) | Wordt loginformatie over de werking van het algoritme bewaard en toegankelijk gemaakt? | |
| **4.02** | Toegangsrechten niet meer up-to-date | Wordt gecontroleerd of toegangsrechten up-to-date zijn met betrekking tot de omgeving waarin het algoritme functioneert? | 2.2 |
| **4.03** | Onrechtmatige toegang tot het algoritme | Worden toegangsrechten aangepast zodra er een uitdiensttreding of functiewijziging van een werknemer plaatsvindt? | 2.2 |
| **4.04** | Toegang wordt uitgegeven door persoon die daarvoor niet is geautoriseerd | Worden toegangsrechten uitgegeven door daarvoor bevoegde personen? | 2.2 |
| **4.05** | Kans op manipulatie van het algoritme bij conflicterende toegangsrechten | Wordt functievermenging voorkomen bij de toegang van gebruikers tot het algoritme? | 2.2 |

| Nr. | Risico | Onderzoeksvraag | Ethisch principe |
|---|---|---|---|
| **4.06** | Hoe meer toegewezen speciale bevoegdheden, hoe meer kans op manipulatie | Wordt er gebruikgemaakt van generieke beheeraccounts? Staat het aantal beheeraccounts in logische verhouding tot de beheerders? | 2.2 |
| **4.07** | Gebruikersgroepen van het algoritme lastig te identificeren | Wordt er bij het inrichten van toegangsrechten van verschillende gebruikersgroepen/rollen gebruik-gemaakt van naamgevingsconventies en systematiek? | 2.2 |
| **4.08** | Beheerders en gebruikers van het algoritme lastig te identificeren | Worden er naamgevingsconventies gebruikt voor gebruikers en beheer-ders, zodat zij geïdentificeerd kunnen worden? | 2.2 |
| **4.09** | Onduidelijkheid over wie wijzigingen/ werkzaamheden aan het algoritme heeft uitgevoerd | Voeren beheerders werkzaamheden als beheerder en werkzaamheden als gewone gebruiker uit onder 2 verschil-lende gebruikersnamen? | 2.2 |
| **4.10** | Als er wel toegang is tot onderliggende componenten kan manipulatie van de database plaatsvinden | Hebben gebruikersaccounts wel of geen directe toegang tot onderliggende componenten? | 2.2 |
| **4.11** | Als er toegang is tot onderliggende componenten kan manipulatie van de database plaatsvinden met betrekking tot functiescheiding | Bestaat er een functiescheiding tussen aanvragen, autoriseren en verwerken van wijzigingen in gebruikersaccounts en toegangsrechten? | 2.2 |
| **4.12** | Als er toegang is tot onderliggende componenten kan manipulatie van de database plaatsvinden met betrekking tot wachtwoordbeheer | Is het wachtwoordbeheer interactief en zijn de wachtwoorden van geschikte kwaliteit? | 2.2 |
| **4.13** | Ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies, niet naleven van wetgeving | Worden wijzigingen in de code van het algoritme op een gecontroleerde wijze uitgevoerd? Denk aan het testen en accorderen/autoriseren van wijzigingen | 2.2 |
| **4.14** | Ongeautoriseerde toegang en daarmee kans op manipulatie van het algoritme (wijziging, beschadiging, dataverlies) | Is het algoritme beveiligd, zodat er geen risico is op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies? | 2.2 |
| **4.15** | Back-ups zijn niet in overeenstemming met het back-upbeleid. Er is geen hersteloptie bij uitval van het algoritme en er is risico van gegevensverlies | Worden er back-ups van het algoritme gemaakt en kunnen het algoritme en de data hersteld worden? | |
| **4.16** | Bij het ontbreken van *security by design* zijn er risico's | Is er sprake van security by design? | 2.1 |

# Bijlage 4 Afkortingen en begrippen

| | Omschrijving |
|---|---|
| **Algoritme** | 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 |
| **Bias** | Onwenselijke systematische afwijking voor specifieke personen of groepen |
| **CAS** | Criminaliteits Anticipatie Systeem |
| **CBR** | Centraal Bureau Rijvaardigheidsbewijzen |
| **CJIB** | Centraal Justitieel Incassobureau |
| **DG Migratie / DGM** | Directoraat-generaal Migratie van het Ministerie van Justitie en Veiligheid (JenV) |
| **Toeslagen** | Directoraat-generaal Toeslagen van het Ministerie van Financiën |
| **DPIA** | Data Protection Impact Assessment, ofwel een gegevensbeschermingseffectbeoordeling |
| **IT-beheer** | Basisbeheersmaatregelen die organisaties treffen om IT-systemen te beveiligen en te beheersen: toegangsbeveiliging, wijzigingenbeheer en back-up en recovery |
| **Model en data** | De ontwikkeling en het onderhoud van het algoritme |
| **PGB** | Persoonsgebonden budget |
| **Procedurele transparantie** | Eigenaren van een algoritme moeten verantwoording afleggen over de gevolgde procedure bij de totstandkoming en de uitkomsten van het algoritme |
| **RvIG** | Rijksdienst voor Identiteitsgegevens |
| **RVO** | Rijksdienst voor Ondernemend Nederland |
| **rwt** | Rechtspersonen met een wettelijke taak zijn zelfstandige organisaties op afstand van de rijksoverheid |
| **SLA** | Service Level Agreement |
| **Sturing en verantwoording** | Het vastleggen van verschillende elementen: de rollen, verantwoordelijkheden en deskundigheid, risico-afwegingen bij het gebruik van het algoritme en afspraken met externe partijen over bijvoorbeeld aansprakelijkheid |
| **SVB** | Sociale Verzekeringsbank |
| **SyRI** | Systeem Risico Indicatie |
| **Technisch complexe algoritmes** | Algoritmes die technisch complex zijn, zoals beeldherkennings-systemen en lerende algoritmes |
| **Technisch eenvoudige algoritmes** | Algoritmes die technisch eenvoudig zijn zoals beslisbomen, zoekmachines en data-uitwisselingssystemen |

| | Omschrijving |
|---|---|
| **Technische transparantie** | Eigenaren van een algoritme moeten de werking ervan kunnen uitleggen |
| **TVL** | Tegemoetkoming Vaste Lasten, een financiële regeling om ondernemers tegemoet te komen die omzetverlies lijden door de coronamaatregelen. |
| **TVS** | Toeslagenverstrekkingensysteem |
| **zbo** | Zelfstandig bestuursorgaan |

# Bijlage 5 Eindnoot

In het conceptrapport stond vermeld dat de Rijksdienst voor Identiteitsgegevens (RvIG) helemaal geen openbaar privacybeleid heeft. Omdat de RvIG ons na het versturen van ons conceptrapport heeft aangetoond dat zij wel degelijk een openbaar privacybeleid heeft, is deze passage verwijderd.

**Algemene Rekenkamer**
Afdeling Communicatie
Postbus 20015
2500 EA  Den Haag
070 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

De tekst in dit document is
vastgesteld op 13 mei 2022.
Dit document is op 18 mei 2022
aangeboden aan de
Tweede Kamer.

Foto omslag: Shutterstock.

**Den Haag, mei 2022**