



Gegevensbeschermingseffectbeoordeling (GEB)

Doelgericht ingrijpen op een aangevraagde toeslag (M1354): Het Risicoclassificatiemodel

Ministerie van Financiën, directie Toeslagen

Utrecht, maart 2021



Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Typ naam/functie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Typ naam/functie

Advies Selecteer/typ datum

Naam: Typ naam/functie

Gegevensbeschermingseffectbeoordeling (GEB)

Ministerie van Financiën, directie Toeslagen
Directie Toeslagen

Contact:

Ministerie van Financiën, directie Toeslagen

Contact Persoon:

Versie: 2.0

Inhoudsopgave

Inleiding.....	5
A. Beschrijving kenmerken gegevensverwerkingen.....	6
1. Voorstel	6
2. Persoonsgegevens	6
3. Gegevensverwerkingen	8
4. Verwerkingsdoeleinden	12
5. Betrokken partijen	14
6. Belangen bij de gegevensverwerking	15
7. Verwerkingslocaties	15
8. Techniek en methode van gegevensverwerking	16
9. Juridisch en beleidsmatig kader	36
10. Bewaartermijnen	37
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	38
11. Rechtsgrond	38
12. Bijzondere persoonsgegevens	39
13. Doelbinding	40
14. Noodzaak en evenredigheid	40
15. Rechten van de betrokkene	43
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	45
16. Risico's	45
D. Beschrijving voorgenomen maatregelen.....	49
17. Maatregelen	49
Bijlage 1: Bronnen	
Bijlage 2: Halfproducten	
Bijlage 3: HT indicatoren	
Bijlage 4: KOT indicatoren	
Bijlage 5: Control Matrix	
Bijlage 6: Instemming verzoek monitoring OR	
Bijlage 7: AU processen	

Inleiding

Per 25 mei 2018 is de General data protection regulation (GDPR) in werking getreden. Beter bekend als de Algemene verordening gegevensbescherming (AVG). In deze wet is vastgelegd dat het verplicht is om een Gegevensbeschermingseffectbeoordeling (hierna: GEB) uit te voeren.

Het doel van een GEB is om privacyrisico's in kaart te brengen van nieuwe projecten en initiatieven of bestaande verwerkingen van persoonsgegevens. Het draagt bij aan het vermijden of verminderen van privacyrisico's. Door middel van een GEB wordt op systematische wijze inzichtelijk gemaakt hoe groot de kans is dat de privacy van betrokkenen geschaad wordt en welke maatregelen er nodig zijn. Na het uitvoeren van de GEB heeft de organisatie antwoorden op deze vragen en kan er op deze basis een proces beschreven worden over de te nemen maatregelen als er zich calamiteiten of incidenten voordoen.

Deze GEB is uitgevoerd bij directie Toeslagen. Voor deze GEB wordt het proces "doelgericht ingrijpen op een aangevraagde toeslag" (binnen Toeslagen benoemd het risicoclassificatiemodel) beschreven zoals dat bij Toeslagen gebruikt wordt. Het Risicoclassificatiemodel (RCM) wordt ingezet om een inschatting te maken van het risicogehalte van toeslagaanvragen, oftewel de kans dat een aanvraag na controle aangepast of afgekeurd moet worden. Deze risicoclassificatie helpt Toeslagen bij het maken van behandelkeuzes zoals bijvoorbeeld meteen uitbetalen of eerst bewijsstukken opvragen. Deze verwerking valt onder de hoofdverwerking Toezicht.

Op basis van art. 35 AVG is deze GEB vereist omdat de volgende criteria van toepassing zijn:

- a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

De AP¹ geeft aan dat het uitvoeren van een GEB verplicht is voor bepaalde verwerkingen. Op het proces "doelgericht ingrijpen op een aangevraagde toeslag" zijn de volgende criteria van toepassing:

- Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens in het kader van fraudebestrijding.
- Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen.
- Profilering

De onderstaande criteria, die afkomstig zijn van de Europese Privacy-toezichthouder, de European Data Protection Board (EDPB), zijn van toepassing:

- Evaluatie of scoretoekenning.
- Matching of samenvoeging van datasets
- Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen
- Op grote schaal verwerkte gegevens

¹ Autoriteit Persoonsgegevens

De volgende artikelen van het Handvest van de Grondrechten van de EU worden ook op één of andere manier geraakt door de verwerkingen die vallen onder het proces "doelgericht ingrijpen op een aangevraagde toeslag":

Artikel 8: Bescherming van persoonsgegevens

Artikel 20: Gelijkheid voor de wet

Artikel 41: Recht op behoorlijk bestuur

Artikel 48: Vermoeden van onschuld en rechten van de verdediging

Deze GEB wordt minimaal eens in de 3 jaar, of bij grote wijzigingen herijkt. Het gaat dan om wijzigingen aan het proces of aan systemen. Het proces van herijken werkt als volgt. In een multidisciplinaire workshop wordt getoetst of de GEB nog de werkelijke verwerking c.q. situatie beschrijft. Daarnaast wordt gekeken naar de verwerkte gegevens en of de gegevens nog proportioneel en subsidiair zijn. Verder wordt de risicoanalyse voor betrokkenen opnieuw gemaakt en toetsen we de maatregelen in de actualiteit.

Na dit proces wordt er een addendum toegevoegd aan de GEB en voorgelegd aan het Management Team DGT ter akkoord en opvolging van de maatregelen. De GEB krijgt dan een nieuwe datum en versienummer. Afhankelijk van de inhoud wordt er advies gevraagd aan de Functionaris Gegevensbescherming en Privacy Officer. Vervolgens wordt er binnen de implementatie getoetst in hoeverre de maatregelen zijn doorgevoerd. Deze evaluatie volgt na 1 jaar nadat de GEB is vastgesteld. De evaluatie wordt gedaan door medewerkers van BDO/Bedrijfsvoering, het team Integrale beveiliging en Privacy (IBP Toeslagen).

A. Beschrijving kenmerken gegevensverwerkingen

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

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

1. Voorstel



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

[Klik hier om infotekst te verbergen](#)

Om een PIA te kunnen verrichten moet duidelijk zijn op welk onderwerp/object deze betrekking heeft. Met een korte en bondige beschrijving van het voorstel waar de PIA op ziet, wordt tevens voorkomen dat bij het nalopen van de 17 punten hier verschillend over wordt gedacht. Ten behoeve van de duidelijkheid kan het nuttig zijn om expliciet aan te geven waar de PIA niet over gaat. Bij conceptregelgeving kan voor deze beschrijving van het voorstel aansluiting worden gezocht bij het voorlopige ontwerp van de inleidende paragraaf van de memorie of nota van toelichting bij het voorstel, voor zover deze betrekking heeft op verwerkingen van persoonsgegevens. Bij

overheidsverwerkingen kan in hoofdlijnen worden beschreven hoe de gegevensverwerkingen er uit zullen zien. Als dat er is kan worden aangesloten bij het projectvoorstel of een beschrijving van de architectuur.

De missie van de directie Toeslagen is het juist, tijdig en rechtmatig uitbetalen van toeslagen. Om dit zo efficiënt mogelijk te doen is handhaving onmisbaar. Wij willen daarbij maatwerk leveren door de juiste combinatie van dienstverlening, voorkomen van fouten, toezicht en fraudebestrijding. Toekenningszekerheid in een zo vroeg mogelijk stadium is een belangrijk onderdeel van deze strategie.

Maandelijks verwerkt directie Toeslagen² honderdduizenden mutaties in toeslagaanvragen. Periodiek (ongeveer eens per maand) worden alle mutaties in een keer beschikt: de wijziging in de aanvraag wordt effectief gemaakt door een formele beschikking aan te maken. Na een formele beschikking wordt de toeslag uitgekeerd.

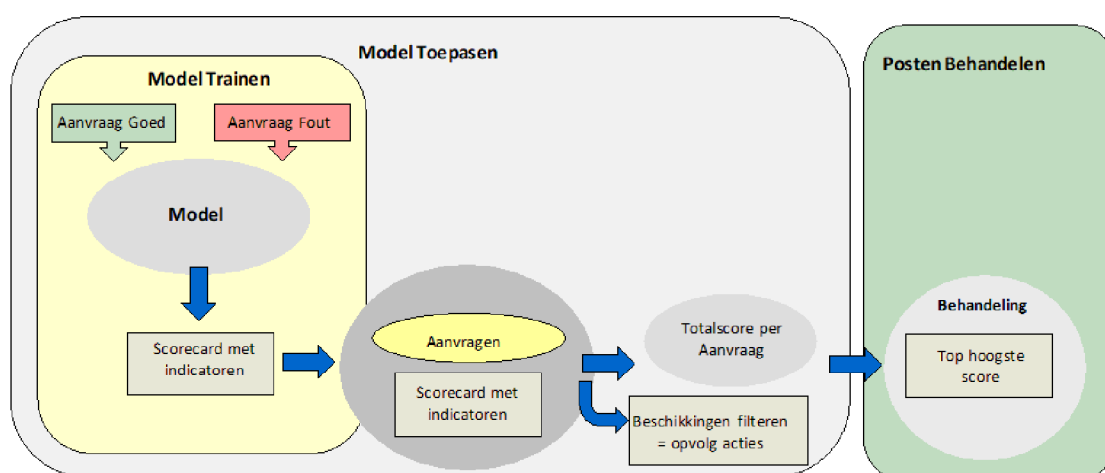
Om grip te houden op mogelijke foutieve aanvragen en mutaties, wordt vlak voor het periodieke beschikkingsproces voor alle aanvragen (waarvoor een conceptbeschikking is afgegeven) een risicoscore berekend door middel van een lerend risicoclassificatie model. Deze score drukt de kans uit dat een aanvraag volgens het model onjuist is. De aanvragen met de hoogste risicoscore worden aangeboden aan behandelaars van de Toezicht team voor handmatige controle op juistheid. Het proces waarmee deze risicoscore berekend en opgevolgd wordt heet risicoclassificatie.

Het Risicoclassificatie model wordt toegepast voor Huurtoeslag en Kinderopvangtoeslag, afhankelijk van de indicatoren die worden gebruikt in het model.

Het Risicoclassificatiemodel wordt getrained volgens de supervised learning³ methode. Dat betekent dat het model leert van bekende voorbeelden van rechtmatig/onrechtmatig gebruik en de geleerde kennis toepast op onbekende cases.

Het Risicoclassificatie proces bestaat uit 3 onderdelen:

- A. Het trainen van het model;
- B. Het toepassen van het model en het filteren van beschikkingen (opvolgacties);
- C. Het behandelen van de geselecteerde posten.



² Belastingdienst/Toeslagen

³ https://en.wikipedia.org/wiki/Supervised_learning

Onderdelen A en B worden verder in deze GEB geanalyseerd. Onderdeel C maakt al deel uit van GEB M8776 Toezicht en zal hier dus niet in detail behandeld worden.

Het proces raakt ook andere processen die betrokken zijn in andere GEB's, zoals:

M8776 Toezicht

M861 Behandeld Fraudesignalen

M2077 Handmatige behandeling van onvolledige en/of tegenstrijdige toeslagenaanvragen (Uitval/uitworp)

M860 Handmatig behandelen aanvragen Toeslagen (Uitval/Uitworp)

M675 Definitief Toekennen Toeslag

Hoe het risicoclassificatie proces begint

HHR geeft opdracht aan DAT om een bepaald aantal toeslagaanvragen te selecteren met de hoogste kans op fouten. Het aantal posten wordt bepaald aan de hand van de beschikbare behandelcapaciteit en er wordt bepaald waar aanvragen aan moeten voldoen om in aanmerking te komen voor selectie door het model (selectie van de indicatoren). De indicatoren zijn variabelen zoals aantal kinderen, leeftijd, huurprijs, etc.

Hoe het model wordt getraind

Het risicoclassificatiemodel is een zelflerend model dat wordt getraind door het toevoegen van goede (rechtmatig) en foute (onrechtmatig) aanvragen. De selectie van goede en foute cases wordt gebaseerd op eerdere behandelingen of ervaringen. De trainingcases bevatten alleen BSN nummers, maar om het model te kunnen trainen zijn meer gegevens nodig. Die extra gegevens zijn de indicatoren die uit verschillende bronnen komen (halfproducten en beschikkingen). De indicatoren worden geselecteerd tijdens brainstormsessies tussen HHR en de behandelaars van het Toezicht team. Die selectie is gebaseerd op huidige en eerdere ervaringen uit het toezichtpraktijk. Het model wordt gevoed door het bestand met de datapreparatie in SAS te verwerken; op die manier wordt het model getraind. Tijdens dit proces wordt er bepaald welke indicatoren voorspellen of een aanvraag goed of fout gekeurd wordt en hoe zwaar deze indicatoren wegen. Het resultaat is een scorecard met te beoordelen indicatoren en hun gewicht. Met de beschikbare scorecard worden later alle aanvragen getoetst door het model. Randvoorwaarden voor een betrouwbare scorecard zijn een frequente toevoer van nieuwe testcases zodat het model blijft leren van data die representatief is.

Hoe het model wordt toegepast

Op de scorecard krijgt elke indicator een bepaalde score toegewezen. Om het model te draaien zijn gegevens van alle aanvragen nodig. De input voor het model zijn de gegevens die gerelateerd zijn aan de indicatoren van de scorecard. Het model wordt daarna in SAS gedraaid.

Het Risicoclassificatiemodel toetst alle aanvragen in een maand aan de hand van de scorecard.

Elke indicator op de scorecard heeft een waarde⁴ en deze waarde resulteert voor iedere aanvraag in een uiteindelijke totaalscore die wordt gebruikt als risicoscore.

De aanvragen met de hoogste risicoscore (ongeveer 30 per maand, afhankelijk van beschikbare capaciteit) worden aangeboden aan behandelaars van het Toezicht team voor handmatige controle op juistheid. De rest van de aanvragen krijgen een formele beschikking.

Behalve de risicoscore zijn er nog een aantal kenmerken van de aanvraag die bepalen wat er met de conceptbeschikking gebeurt. Deze kenmerken worden per toeslagaanvraag in het model vastgesteld. Vervolgens wordt aan de hand van deze kenmerken per aanvraag bepaald wat de relevante opvolgactie is (bijvoorbeeld uitworp of VT/DT proces).

⁴ Bijvoorbeeld: Het model beslist dat de indicator 'aantal kinderen' in combinatie met de indicator 'afstand KOO' een hogere score opleveren; dit is gebaseerd op de informatie van onrechtmatige aanvragen die onderdeel is van de trainingcases. Het kan bijvoorbeeld blijken dat aanvragen met minder dan 3 kinderen en meer dan 25 km afstand hoger scoren dan andere aanvragen.

Het streven van directie Toeslagen is om 95% van de toeslagenaanvragen en wijzigingen volledig geautomatiseerd af te handelen. Als dat niet lukt is handmatige behandeling nodig. Daarom wordt vóór de start van het massale automatische continuering (MAC) proces het risicoclassificatiemodel toegepast. Bij aanvragen waaraan een hoog risico wordt toegekend is handmatige behandeling nodig. Deze aanvragen worden voorlopig van het MAC-proces uitgesloten.

2. Persoonsgegevens



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

[Klik hier om infotekst te verbergen](#)

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer wel een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende

eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele

gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtkenummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- b. personen die voor een strafbaar feit zijn veroordeeld;
- c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij conceptregelgeving kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

De gegevens die worden verwerkt binnen het risicoclassificatiemodel zijn afkomstig uit verschillende externe bronnen. Met die gegevens worden halfproducten gemaakt die worden gekoppeld aan beschikkingen. Die datapreparatie wordt gebruikt om het model te trainen en toe te passen. Het aantal persoonsgegevens dat wordt gebruikt binnen de datapreparatie is afhankelijk van de indicatoren die geselecteerd worden.

Gewone persoonsgegevens

ID	Veldnaam	Bron1 ⁵	Bron 2 ⁶	Betrekking	Relevant voor onderdeel
1	NAW gegevens: - Postcode en Huisnummer - Woonland - Postadres, Adres woning	BRP ⁷ , CIV ⁸		Av ⁹ , Tp ¹⁰	A, B, C
2	Persoonlijke gegevens: - Geboortedatum - Leeftijd - Aantal kinderen - Overlijdensdatum	BRP, FLG ¹¹ (CIV)		Av, (Tp, Mb ¹² en kind voor geboortedatum)	A, B, C
3	Inkomen gegevens: - Bijstand (WWB-uitkering)* - Inkomen - Dagtaak - Draagkracht	FLG (CIV)	Av, Tp, Mb	Av, Tp	A, B, C
4	Huurtoeslag gegevens: - Huurprijs woning - soort woning - Dienst en Recreatieruimten kosten - Energiekosten, - Rekenhuur - Schoonmaakkosten - Standplaatsuur - Woonobject identificatie - Maximale huurgrens	VHA ¹³	Av	Av	A, B, C

⁵ Externe bronnen behalve TVS, trainingcases en intensief toezicht die interne bronnen zijn.

⁶ Gegevens worden door de aanvrager zelf verstrekt.

⁷ Basisregistratie Persoonsgegevens

⁸ Centraal Informatie Voorzieningen

⁹ Aanvrager

¹⁰ Toeslag Partner

¹¹ Fiscale Loon Gegevens

¹² Medebewoner

¹³ Verhuurders Administratie

¹⁴ Algemene Kinderbijslagwet

¹⁵ Sociale Verzekeringsbank

	basis van de AKW ¹⁴ **				
6	Gegevens KOO ¹⁶ : • Naam • Adres en plaats opvanglocatie en gastouderbureau • Aantal uren opvang • Ingangsdatum kinderopvangtoeslag • periode waarop het kind kinderopvang heeft • uurtarief • soort opvang (dag-/of buitenschools, kindercentrum of gastouder) • LRK-id van opvanglocatie	SZW (LRK) ¹⁷ , CIV, DUO	Av	Av, KOO	A, B, C
7	Aanvraag gegevens: • Type regeling • Ingangsdatum aanvraag • Wijzigingen van de aanvraag op datum en tegemoetkomingsjaar • Product- en procesresultaten van de behandeling van de aanvraag zoals de hoogte van de toeslag (beschikking).	CIV	Av	Av	A, B, C
8	Huishouden gegevens	Directie Toeslagen (TVS)		Av	A, B, C
9	Persoonsrelaties: • Ouder kind relatie	CIV	Av	Av, Kind	A, B, C
10	Nederlandschap*	BRP		Av	A, B
11	Status voorderingen en beschikkingen: • Toeslagjaar • Beschikkings-nummer • Datum-dagtekening • Jaarbedrag	CIV			
12	Wanbetaler zorg status*	CVZ ¹⁸ (CIV)		Av	A, B
13	WOZ onroerend goed bezitting	CIV		Av	A, B, C
14	Medewerkers ID	ICT Infra logging		Medewerker	A, B, C

* Deze gegevens (WWB-uitkering, Nederlandschap, Wanbetaler zorg status) worden niet meer als indicator gebruikt maar ze maken nog steeds deel uit de datapreparatie. Ze zullen in Q2 2021 structureel uit de datapreparatie verwijderd worden (zie Risico's en maatregelen).

¹⁴ Algemene Kinderbijslagwet

¹⁶ Kinderopvang Organisatie

¹⁷ Ministerie van Sociale Zaken en Werkgelegenheid

¹⁸ College voor Zorgverzekeringen

**Het gegeven "Recht op kinderbijslag op basis van de AKW" is gerelateerd aan de KGB¹⁹ regeling en niet aan KOT of HT. Het gebruik kan onrechtmatig zijn, daarom is het als een risico geregistreerd (zie 16.Risico's, risico 2.)

Wettelijke identificerend persoonsgegevens

Id	Veldnaam	Bron 1	Bron 2	Betrekking op	Relevant voor onderdeel
15	BSN ²⁰	BVR, DUO ²¹ , COA ²² , CIV, TVS, trainingcases, toezichtlijst ²³	Av	Av, Tp, Mb, Kind	A, B, C

3. Gegevensverwerkingen



Geef alle voorgenomen gegevensverwerkingen weer.

[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Denk hierbij aan:

het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Indien mogelijk verdient het aanbeveling om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een *input-proces-output* model, *flowchart* of *workflow*.

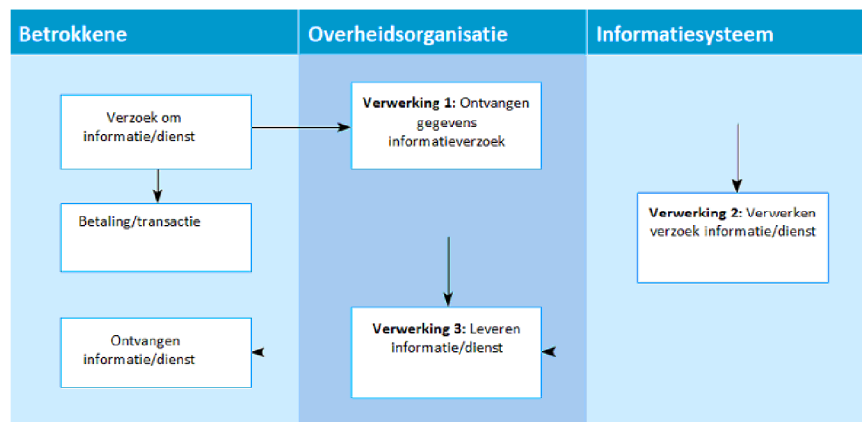
¹⁹ Kinderbondbudget

²⁰ Burgerservicenummer

²¹ Dienst Uitvoering Onderwijs

²² Centrale Ontvangers Administratie

²³ Lijst met BSN's die bevat de bewezen fraudegevallen behandeld door het IntensiefToezichtteam



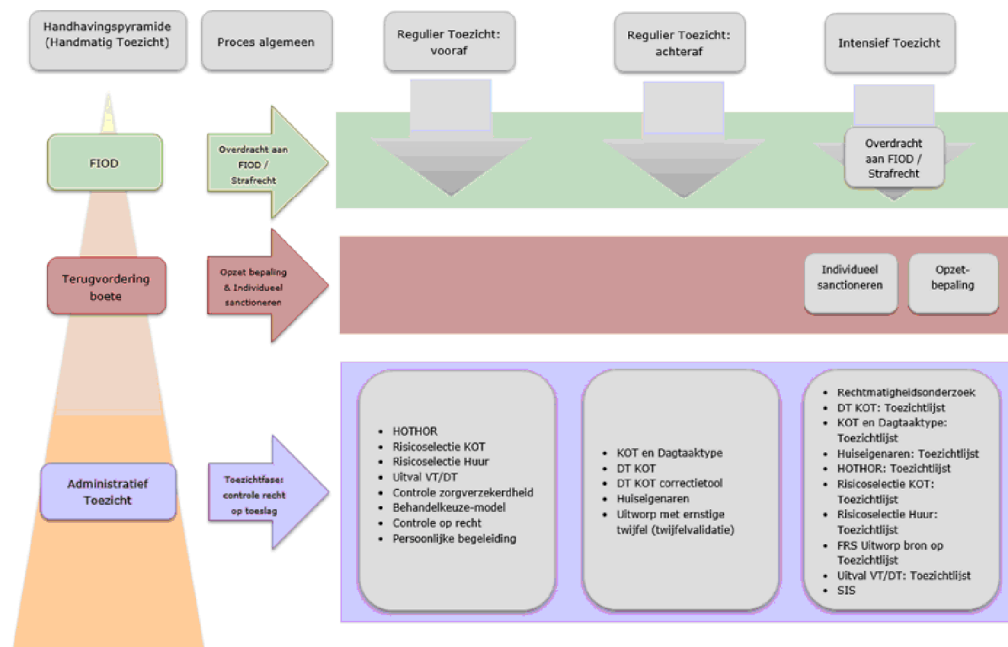
Het proces "doelgericht ingrijpen op een aangevraagde toeslag" valt onder de Toeslagen bedrijfsprocessen 'Toezicht – handavingsregie'. De Belastingdienst beoogt met 'handhaving' het gedrag van burgers en bedrijven zodanig te beïnvloeden dat zij structureel (fiscale) regels naleven (compliance). Dit moet zorgen voor de borging van de continuïteit van belastingopbrengsten en de rechtmatige betaling van toeslagen. Directie Toeslagen handelt bij het handhaven binnen de juridische kaders van de wet en conform de beginselen van behoorlijk bestuur.

Onder handhaving wordt door directie Toeslagen alle activiteiten verstaan die bijdragen aan structurele regelnaleving (compliance) door toeslaggerechtigden. Dit houdt voor directie Toeslagen specifiek in dat de burger

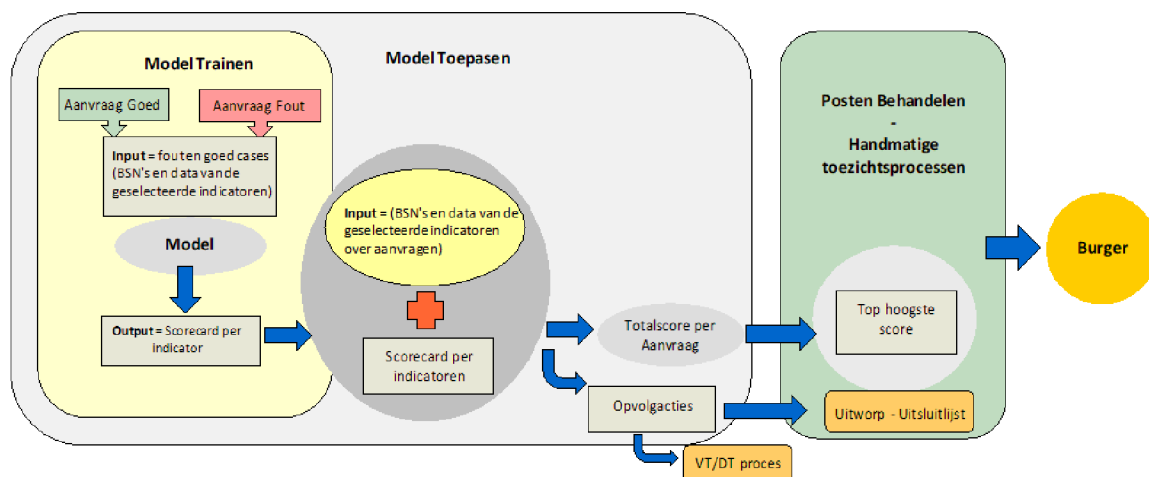
- (a) juiste en volledige informatie verstrekt bij de aanvraag van een toeslag en bij het doorgeven van wijzigingen die relevant zijn voor de aanspraak op een toeslag,
- (b) tijdig en adequaat reageert op verzoeken van de directie Toeslagen om informatie en
- (c) eventuele terugvorderingen tijdig betaalt.

In aanvulling op deze algemene compliance doelstelling streeft directie Toeslagen met haar handavingsbeleid het waarborgen na van de rechtmatigheid van de toekenning van toeslagen, ofwel de mate waarin wordt gehandeld in overeenstemming met de geldende wet- en regelgeving.

Onderstaand is ingezoomd op de handmatige toezichtsprocessen:

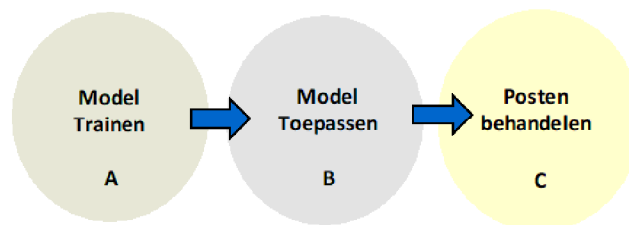


De output van het risicoselectiemodel (risicoclassificatiemodel) wordt gebruikt binnen het handmatige toezichtsproces van administratief Toezicht. Hieronder wordt ingezoomd op de verwerking zelf:



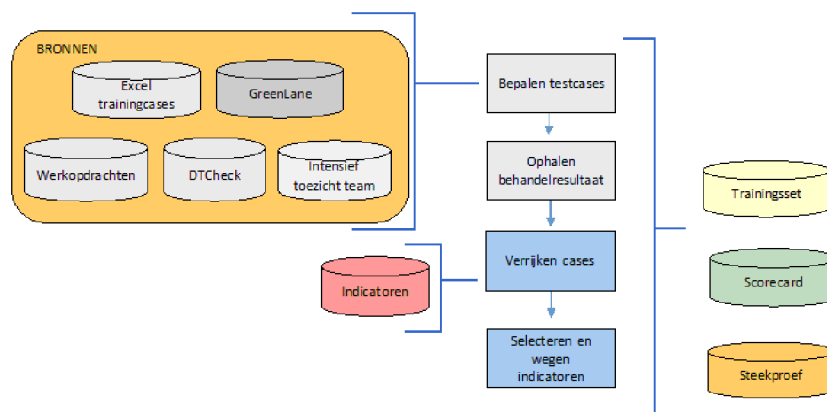
Het risicoclassificatiemodel proces bevat 3 onderdelen:

- Het trainen van het model
- Het toepassen van het model en het bepalen van opvolgacties
- Het behandelen van de geselecteerde posten



De GEB is ingedeeld volgens deze driedeling, waarbij dus alleen onderdeel A en B beschreven worden in deze GEB.

A. Trainen van het model



Het RCM is 'lerend': aan de hand van aanvragen uit het verleden waarvan bekend is of deze fout (onrechtmatig) of goed (rechtmatig) waren. Dit is bekend als zijnde de 'trainingscases'. Hierbij wordt uitgerekend welke combinaties van indicatoren risicovol zijn.

De trainingscases vormen het ruggengraat van de risicoclassificatiemodel: zonder een gebalanceerde populatie van kwalitatief goede trainingscases is het onmogelijk een goed model te trainen, en hierop in beleid en uitvoering op te steunen.

Doel van de trainingscases proces is om de toevoer van goede trainingscases te continueren. Hierdoor wordt de trainingset geleidelijk ververs, en groeit het model automatisch mee met de patronen van niet compliant cases die recent geconstateerd zijn.

Het model wordt gevoed met trainingscases waaraan historische contra-informatie toegevoegd wordt. Deze reconstructie van trainingscases wordt 'tijdreizen' genoemd.

Alleen wanneer nieuwe trainingscases geïdentificeerd worden zal het tijdreizen aangepast en opnieuw gerund moeten worden. Wanneer geen nieuwe trainingscases beschikbaar zijn zal de trainingset, en daarmee ook het model, gelijk blijven.

Er worden vijf bronnen voor de trainingscases gebruikt:

1. Trainingscases in Excel

2. GreenLane
3. Werkopdrachten (TVS)
4. Intensief toezicht teams
5. DTCheck

Er wordt per bron bepaald of het behandelresultaat goed of fout is geweest. De bronnen bevatten BSN nummers van aanvragen uit het verleden waarvan bekend is dat deze fout (onrechtmatig) of goed (rechtmatig) zijn geweest. Voor elke bron zijn businessrules opgesteld die bepalen wanneer een case 'fout' of 'goed' genoemd wordt. (zie hoofdstuk 8. Techniek en methode van gegevensverwerking - 2. Bepalen behandelresultaat (goed / fout))

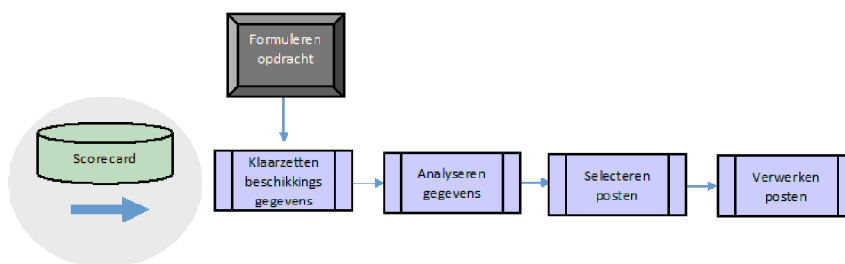
Aan de trainingscases voegt DAT gegevens over de aanvraag en aanvrager toe die pas in de vervolgstap worden geanalyseerd op voorspellende kracht. Dit zijn de indicatoren die gebruikt worden om het scoremodel te bepalen.

De indicatoren zijn variabelen (bijvoorbeeld: aantal kinderen of aantal verhuizingen) die een indicatie kunnen zijn of onrechtmatigheid. De indicatoren zijn geselecteerd door HHR en PR op basis van eerdere onrechtmatige cases. De informatie die gerelateerd is aan de indicatoren komt uit verschillende bronnen (halfproducten en beschikkingen, zie hoofdstuk 8. Techniek en methode van gegevensverwerking - 3. Klaarzetten beschikking gegevens) en wordt aan het BSN gekoppeld. Dit bestand met BSN's en gekoppelde informatie van de geselecteerde indicatoren wordt gebruikt om het model te kunnen trainen. De verschillende versies van dit bestand worden in SAS opgeslagen. Alleen geautoriseerde DAT medewerkers hebben toegang tot het bestand.

Maar er zijn een aantal oude SAS bestanden die ook op de Q-schijf worden bewaard. Dit stamt nog uit de tijd dat we niet de beschikking hadden over de SAS Grid en alles nog op een aparte pc op moesten slaan. Die bestanden moeten nog bewaard worden om het model te kunnen trainen, maar het is niet meer nodig om die bestanden op de Q-schijf te bewaren - het kan ook alleen op de SAS Grid. Dit zal in 2021 worden aangepast (zie Risico 9 in Hoofdstuk 16 en 17 Risico's en Maatregelen)

Door middel van een logistisch regressiemodel wordt er tijdens het trainen van het model een scorecard gemaakt. Deze scorecard bevat de indicatoren met hogere scores die daarna worden gebruikt om de risicoscore van de aanvragen te bepalen.

B. Toepassen van het model



De opdrachtgever HHR²⁴ wil data inzetten om risicogebaseerd keuzes te maken over de aan te bieden posten voor toezichtbehandeling in de fase van voorlopige toekenning: de posten waar het

²⁴ Handhavingsregie

risico het grootst is dat de aanvraag/wijziging niet juist en/of rechtmatig is. De opdrachtnemer D.A.T. maakt hiervoor gebruik van het risicoclassificatiemodel waarin door middel van meerdere indicatoren het risico wordt bepaald of een aanvraag (deels) onrechtmatig is. Vergelijkbaar met het trainen van het model selecteert HHR een aantal indicatoren die worden gekoppeld aan de BSN's van alle lopende en nieuwe aanvragen. De verschillende versies van dit bestand worden in SAS opgeslagen. Zoals net bij A benoemd zijn er een aantal oude SAS bestanden op de Q-schijf opgeslagen en dit zal in Q2 2021 aangepast worden. Alleen geautoriseerde DAT medewerkers hebben toegang tot het bestand.

De toepassing van het risicoclassificatiemodel resulteert in een rangschikking van de aanvragen op basis van de risicoscore.

Samen met de selectie op basis van harde criteria (zie hoofdstuk 8. Techniek en methode van gegevensverwerking - 5.1 Filteren beschikkingen – opvolgacties) wordt de top van deze rangschikking voor handmatige behandeling aangeboden aan toezichtmedewerkers (team Toezicht). In deze behandeling wordt de aanvraag gecontroleerd op het rechtmatig en juist toekennen van de toeslag voordat er een voorlopige toekenning wordt afgegeven.

De teams van Toeslagen die betrokken zijn bij het Risicoclassificatiemodel zijn: HHR in de rol van opdrachtgever, D.A.T. in de rol van opdrachtnemer en Toezicht in de rol van behandelaar van de te controleren posten (uitvoering).

C. Het behandelen van de geselecteerde posten.

Het Toezicht team zal als behandelaar de geselecteerde posten controleren. De verwerking van de bovengenoemde gegevens heeft als verwerkingsdoel het vaststellen van de rechtmatigheid van de toekenning. Door het controleren van de lopende toeslag met de ontvangen bewijsstukken van de belanghebbende of contra-informatie van onder andere kinderopvangorganisaties en verhuurder kan worden vastgesteld of de toeslag een aanpassing behoeft. Hiermee wordt zorg gedragen voor een juiste vaststelling van de toeslagen.

De behandelaar kan na het controleren van informatie de aanvraag handmatig corrigeren als de rechtmatigheid geconstateerd is. Vanaf dat moment kan de aanvraag verder verwerkt worden. Onrechtmatige aanvragen zullen een opvolgend proces volgen. Dit proces wordt in meer detail geanalyseerd in andere GEB's zoals M861 Behandelen Fraudesignalen en M8776 Toezicht.

Dit proces C valt binnen de scope van GEB M8776 Toezicht. Hiermee valt het buiten scope van deze GEB en wordt het hier niet verder in detail beschreven.

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen

gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Id	Veldnaam	Verwerkingsdoel
1	Postcode en Huisnummer, Woonland, Postadres, Adres woning	Verwerking van persoonsgegevens in het kader van de uitvoering van hun taak en om uitwisseling te kunnen maken met (authentieke) bronnen. Het adres is nodig om de geografische locatie te bepalen en de afstand tot het opvangadres te berekenen (indicator

2	Geboortedatum, Aantal kinderen, Overlijdensdatum	afst_adr_opvang). Geboortedatum wordt gebruikt om met voldoende zekerheid te kunnen stellen of het echt om de gegevens van persoon X gaat (vergewisplicht). Voor kinderopvangtoeslag zijn de leeftijden 4 en 12 jaar relevant als indicatie om te bepalen of er recht is op kinderopvangtoeslag op basis van dagopvang of op basis van naschoolse opvang ²⁵ . Dit is afhankelijk van of een kind naar school gaat. Voor de huurtoeslag dient de aanvrager meerderjarig te zijn. ²⁶ Voor de huurtoeslag is de leeftijd van belang bij het vaststellen van de hoogte van het recht op huurtoeslag. Ouderenhuishouden, medebewoner en leeftijd van het kind i.v.m. vrijstellingsdeel van het eventuele inkomen.
3	Toeslagpartner heeft werkt, draagkracht, inkomen Toeslagpartner heeft bijstand (WWB-uitkering)*	Om te kunnen bepalen bij welke bron de contra-informatie over gewerkte uren kan worden geverifieerd. Ter bepaling van de draagkracht ²⁷ wordt het toetsingsinkomen ²⁸ , van de toeslagaanvrager, toeslagpartner, kind (>18jaar) en evt. medebewoner in aanmerking genomen. WWB-uitkering (hoogte) werd als risico indicator in het model opgenomen. WWB-uitkering was een fraudesignaal in het verleden.
4	Huurprijs woning, soort woning, Huurprijs woning, soort woning Dienst en Recreatieruimten kosten, Energiekosten, Rekenhuur, Schoonmaakkosten, Standplaatshuur, Woonobject identificatie, Maximale huurgrens	Om te kunnen bepalen of er recht is op huurtoeslag, en de hoogte van de huurtoeslag te kunnen bepalen.
5	Statusgegevens: Tp of Av heeft recht op kinderbijslag op basis van de AKW voor een kind	Deze gegevens zijn nodig omdat het kindgebonden budget afhankelijk is van het recht op kinderbijslag. ²⁹ Het werd als risico indicator in het model opgenomen. Dit gebruik kan onrechtmatig zijn omdat deze gegevens niet aan KOT en HT gerelateerd zijn. Als onderdeel van de maatregelen zal ook de rechtmatigheid van het gebruik onderzocht worden.
6	Gegevens KOO: Naam, Adres en plaats opvanglocatie en gastouderbureau,	Deze gegevens zijn noodzakelijk om vast te stellen of er sprake is van recht op kinderopvangtoeslag en dit te communiceren met

²⁵ In artikel 1.1.1. lid 1 Wko en artikel 1 sub b Besluit kinderopvangtoeslag.²⁶ Artikel 1, lid 1, onder c van de wet op de zorgtoeslag en artikel 8 wet op de huurtoeslag.²⁷ In artikel 7 lid 1 Awir.²⁸ In artikel 8 lid 1 Awir.²⁹ Artikel 2, lid 1 wet op het kindgebonden budget.

	Aantal uren opvang, Ingangsdatum kinderopvangtoeslag, Periode waarop het kind kinderopvang heeft genoten (begin- en einddatum in deze kalendermaand), uurtarief, Soort opvang (dag-/of buitenschools, kindercentrum of gastouder), LRK-id van opvanglocatie	de burger en de KOO in het aanvraag- en mutatieproces. De hoogte van de kinderopvangtoeslag is afhankelijk van het aantal uren kinderopvang per kind in het berekeningsjaar ³⁰ . De hoogte van de kinderopvangtoeslag is afhankelijk van de voor die kinderopvang te betalen prijs ³¹
7	Aanvraag gegevens: Type regeling, Ingangsdatum aanvraag, Wijzigingen van de aanvraag op datum en tegemoetkomingsjaar, Product- en procesresultaten van de behandeling van de aanvraag, zoals de hoogte van de toeslag (beschikking).	Om de periode van recht op toeslag vast te kunnen stellen
8	Huishouden gegevens: aantal personen	Voor het vaststellen van het recht op en de hoogte van een tegemoetkoming zijn het aantal personen op een adres van belang.
9	Persoonsrelaties: Ouder kind relatie	Verwerking van persoonsrelaties ten behoeve van het vaststellen van toeslagpartnerschap en de samenstelling van het huishouden teneinde de toeslagen correct te kunnen vaststellen.
10	Nederlandschap ja/nee*	Het bepalen of sprake is van wel of geen Nederlandschap is van belang om te kunnen vaststellen of een belanghebbende recht heeft op een toeslag. De manier waarop dit werkt is dat er een script naar de bron in BvR kijkt en bepaalt of de waarde van Nederlandschap ja of nee is. Nationaliteit als gegeven wordt niet op een andere manier verwerkt in het proces. Deze gegevens worden ook niet opgeslagen, behalve de output van het script (Nederlandschap ja/nee of 0/1)
11	Status voorderingen en beschikkingen	Om de financiële situatie van de aanvrager te kunnen bepalen.
12	Wanbetaler zorg status*	Gegevens van gevoelige aard. Het werd als risico indicator in het model opgenomen: aanvrager heeft geen zorgpremie afgedragen (hoger risico).
13	WOZ onroerend goed bezitting	Om te kunnen bepalen of er recht is op huurtoeslag, en de hoogte van de huurtoeslag te kunnen bepalen.
14	Medewerkers ID	Gegevens van gevoelige aard. In het kader van login en monitoring van bepaalde acties (zie hoofdstuk 8)

De volgende gegevens worden sinds een aantal jaar geleden niet meer als indicator gebruikt in het model, maar de gegevens worden nog wel verwerkt als bron (ze zijn onderdeel van de datapreparatie):

3. Toeslagpartner heeft bijstand (WWB-uitkering)

10. Nederlandschap ja/nee

12. Wanbetaler zorg status

³⁰ In artikel 1.7 lid 1 sub b ten eerste Wko.

³¹ In artikel 1.7 lid 1 sub b ten eerste Wko.

Deze zullen in 2021 structureel uit het model verwijderd worden (zie Risico's en Maatregelen). Bij de start van de risicoselectie in 2013 is men op zoek gegaan naar mogelijke indicatoren die invloed hebben op het risico op fouten. Deze indicatoren waren daar een aantal van maar omdat ze geen effect op het model hebben (er geen invloed op de risicoscore is gezien tijdens testen) is er besloten om ze niet meer te gebruiken. Ze worden op "reject" gezet in het model. Dat betekent dat het model deze indicatoren of variabele niet meer gebruikt.

Id	Veldnaam	Verwerkingsdoel
15	BSN	Verwerking van persoonsgegevens³² in het kader van de uitvoering van hun taak en om uitwisseling te kunnen maken met (authentieke) bronnen. Om het model te trainen worden trainingscases gebruikt. Die bevatten een lijst van BSN's met het resultaat fout of goed. Daarnaast wordt het model getraind met een lijst met posten die vanwege de opzet niet compliant zijn. Die lijst komt van het Intensief toezicht team en bevat alleen BSN nummers. Het BSN wordt gebruikt als unieke identifier om de cases te kunnen identificeren en te kunnen koppelen aan de informatie uit de indicatoren (meer informatie in hoofdstuk 12. Bijzondere persoonsgegevens).

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de

³² In artikel 10 Wet algemene bepalingen Burgerservicenummer (Wabb).

verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Directie Toeslagen heeft convenanten gesloten met een aantal organisaties. Dit zijn meestal overheidsorganisaties maar dat hoeft niet altijd zo te zijn. Hierbij gaat het om afspraken over:

- de gezamenlijke handhaving van overheidsregelingen
- het onderling uitwisselen van informatie

De overheid wil dat haar organisaties meer samenwerken waardoor de overheid als geheel efficiënter gaat werken. In dat verband wordt onderling ook informatie uitgewisseld. Uiteraard worden daarbij de wettelijke bepalingen strikt in acht genomen zoals bijvoorbeeld de privacyregelingen. De directie Toeslagen hecht aan transparantie en publiceert daarom de samenwerkingsconvenanten met andere organisaties.

Rol	Naam
Verwerkingsverantwoordelijke	Minister van Financiën, voor deze
	Toeslagen, voor deze de algemene
	Toeslagen
Externe verstrekkers	Gemeente, UWV

³³ Verhuurder van tijdelijk woonruimte. Vanuit directie Toeslagen zijn er afspraken gemaakt met verhuurders met meer dan 10 woningen m.b.t. het standaard leveren van diverse gegevens, waaronder in ieder geval de kale huurprijs en indien van toepassing de

³⁴, FLG, VHA, SVB, SZW, CIV, IBS-COA

Interne verstrekkers
CAP³⁵, Intensief toezicht team

Interne verwerker
HHR, DAT, PR³⁶, CAP-UPG³⁷, Toezicht

Interne ontvanger
Werkvoorbereiding
Queryloket
Handhavingsregie (postbus)

6. Belangen bij de gegevensverwerking



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

Het belang van burgers is dat zij tijdig het juiste toeslagbedrag krijgen. Mocht het feit zich voordoen dat zij geen recht hebben, dan is het in het belang van de aanvrager dat deze ook geen voorschot krijgt, zodat er niet onterecht toeslag uitgekeerd wordt en zodat geen terugvordering plaats hoeft te vinden. Daarnaast is de burger erbij gebaat dat hij zo snel mogelijk het juiste toeslagbedrag krijgt en daarbij niet onterecht in lange toezichtprocessen verzeilt raakt.

Het belang van Toeslagen is het juist, tijdig en rechtmatig uitbetalen van toeslagen. Het RCM is daarbij behulpzaam om zo efficiënt en effectief mogelijk de handmatige behandelcapaciteit in te zetten en burgers daardoor ook zoveel mogelijk meteen het juiste toeslagbedrag uit te keren ipv dat achteraf het toeslagbedrag toch anders blijkt te zijn.

Daarnaast speelt het maatschappelijk belang dat er verwacht mag worden dat de overheid zorgvuldig omgaat met en gebruik maakt van gegevens van burgers. De gegevens van burgers op individueel niveau moeten ook inzichtelijk (gemaakt kunnen worden) zijn.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

[Klik hier om infotekst te verbergen](#)

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen

kosten voor serviceposten, of voor een woonwagendplaats. Deze gegevens worden op jaarlijkse basis gedeeld met de Verhuurdersadministratie van directie Toeslagen en worden vervolgens verwerkt in TVS.

³⁴ Uitvoeringsinstituut Werknemersverzekeringen

³⁵ Centrale Administratieve Processen

³⁶ Productieregie

³⁷ CAP-UPG (Unit Productiekwiteit en Gebruiksbeheer)

buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

Uitsluitend in Nederland.

8. Techniek en methode van gegevensverwerking



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

[Klik hier om infotekst te verbergen](#)

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
- berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

- wettelijk is toegestaan; en
- voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

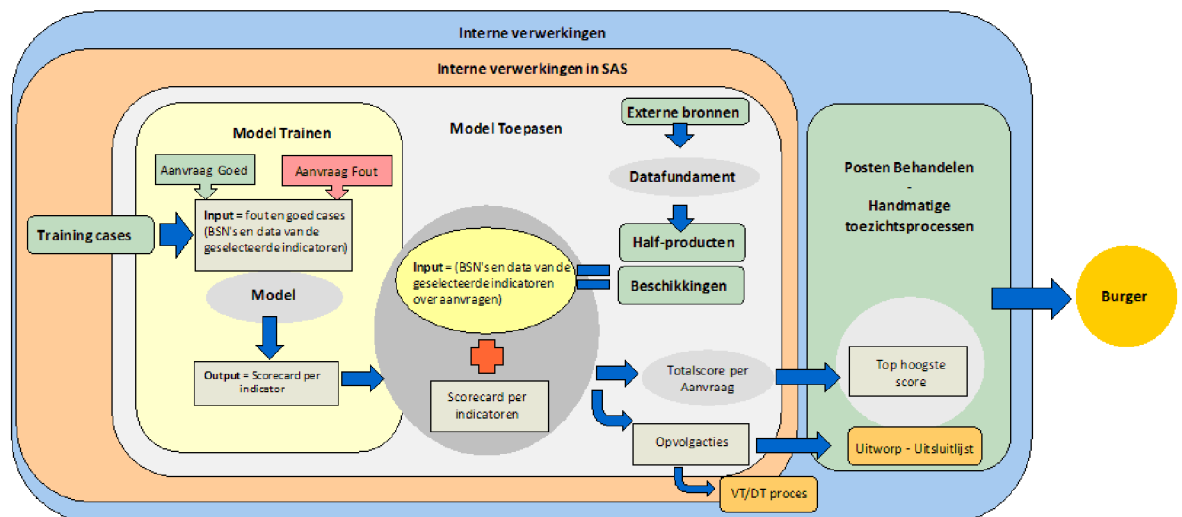
Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

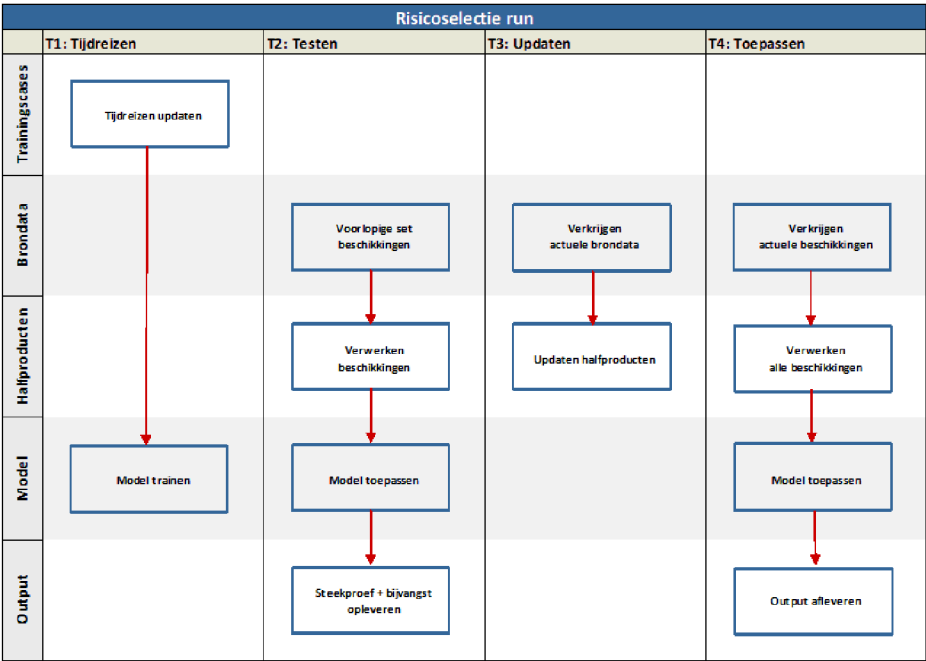
Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

Het risicoclassificatiemodel is lerend en kan op basis van historische aanvragen waarvan de rechtmatigheid/onrechtmatigheid bekend is (trainingscases) de kans voorspellen dat een aanvraag onrechtmatig is. Het model wordt in SAS Enterprise Miner getraind. Tijdens een run van het model wordt in de meeste gevallen eerst een nieuw model berekend. Dit nieuwe model wordt vervolgens toegepast op de meest actuele set beschikkingen. In de praktijk wordt dit niet zo heel vaak gedaan; de huidige scorecard stamt nog uit 2019.



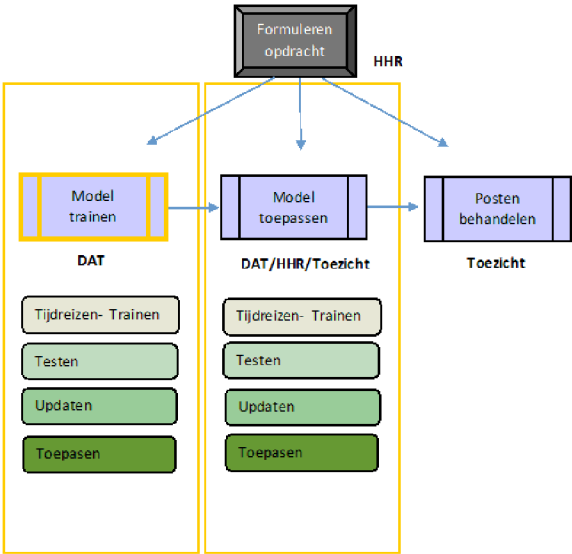
Deze toepassing bestaat uit vier fasen:

1. **Trainen:** de set met trainingscases wordt, indien beschikbaar, aangevuld met nieuwe cases. Het model wordt op basis van de nieuwe trainingsets getraind. Tijden is de samenstelling van de trainingset op basis van historische contra-informatie.
2. **Testen:** het opnieuw getrainde model wordt getest op een voorlopige set van conceptbeschikkingen. Voor de meeste halfproducten wordt hierbij gebruik gemaakt van brondata van de vorige run. Dit leidt tot een steekproef die handmatig beoordeeld wordt door een team medewerkers die fungeren als 'steekproevers'.
3. **Updaten:** de meeste halfproducten worden ververs met actuele brondata. Als de opvolging van steekproef hier aanleiding toe geeft, wordt het model inhoudelijk aangepast. Het model wordt dan nogmaals toegepast, en uit de resultaten wordt wederom een steekproef getrokken.
4. **Toepassen:** alle actuele conceptbeschikkingen worden verkregen en wordt het model voor de laatste keer toegepast. Dit leidt tot definitieve output van het model, op basis waarvan aanvragen stopgezet, onderzocht en gerapporteerd kunnen worden.

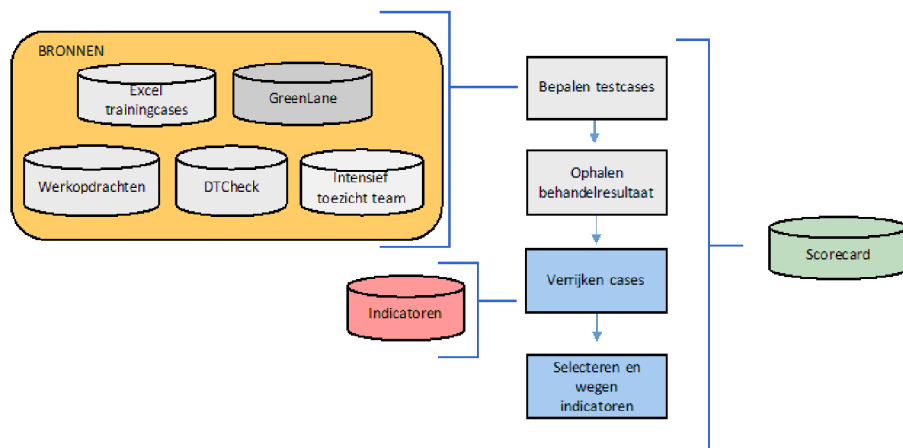


Het RCM proces bevat 3 onderdelen:

- A. Het trainen van het model
- B. Het toepassen van het model en filteren van beschikkingen (opvolgacties)
- C. Het behandelen van de geselecteerde posts



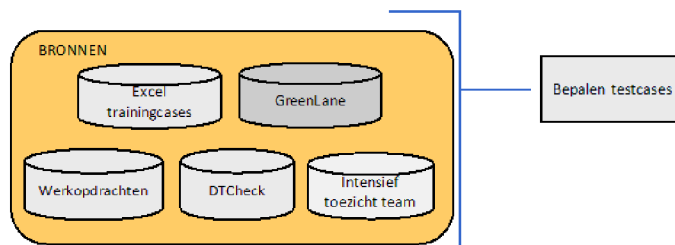
A. Trainen van het model



Proces	Omschrijving	Organisatie
1. Bepalen testcases	Geautoriseerde ³⁸ medewerkers van DAT en HHR bepalen welk type handmatig behandelde aanvragen worden gebruikt als testcase	DAT
2. Bepalen behandelresultaat (goed / fout)	Geautoriseerde medewerkers van DAT geven het label goed of fout aan de testcases	DAT
3. Verrijken cases	Geautoriseerde medewerkers van DAT koppelen indicatoren aan de testcases	DAT, HHR, Toezicht
4. Selecteren en wegen indicatoren	Geautoriseerde medewerkers van DAT bepalen of hoeveel weging de indicatoren hebben in het voorspellen van goed of fout	DAT

1. Bepalen testcases

³⁸ De autorisaties voor het systeem SAS worden door de Teamleader DAT geregeld.



Voor het bepalen van de testcases zijn vijf bronnen beschikbaar die geautoriseerde medewerkers van DAT gebruiken om een trainingsset te vormen waarmee een scorecard gemaakt wordt:

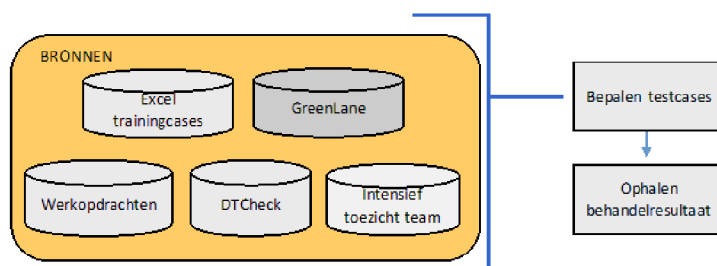
- Trainingscases (Excel bestand):** in het verleden (vanaf mei 2013) zijn handmatig trainingscases verzameld, zowel voor KOT als HT. De oorsprong hiervan is velerlei, en niet altijd vastgelegd. De kwaliteit hiervan is daarom in het algemeen (vooral voor de periode mei – december 2013) wisselend. Ondanks de wisselende kwaliteit vormt deze verzameling posten een substantieel deel van de trainingset. In december 2015 is besloten om cases geïdentificeerd in 2013 te bevroren, en geen nieuwe cases voor toeslagjaar 2013 meer toe te voegen. Daarom worden alle cases met toeslagjaar 2013 of eerder hier al uitgesloten van verdere verwerking. Met ingang van april 2019 zijn ook de jaren 2014 en 2015 bevroren. Sinds 2019 zijn geen cases meer toegevoegd.
De cases zijn in SAS Enterprise tool verwerkt. De output is een Excel bestand die een lijst van BSNs met het resultaat fout of goed bevat. De output is in SAS bewaard. Een backup is ook in een map op de Q-schijf bewaard. Het bestand is toegankelijk voor alle D.A.T. medewerkers.
- GreenLane:** als onderdeel van de GreenLane³⁹ pilots zijn in meerdere iteraties een groot aantal posten behandeld door Toezicht. Deze behandelaars hebben gegeven een groot aantal stukken contra-informatie beoordeeld of deze posten 'de GreenLane op mochten', oftewel: vanwege een laag risico zonder verdere behandeling definitief beschikt mochten worden.
De cases die door de rechters als GreenLane waardig beoordeeld zijn, worden in deze flow als compliant case meegenomen in de trainingset.
Het GreenLane project is gestopt en er worden geen nieuwe trainingscases meer toegevoegd vanuit dit project.
De gegevens (in een onversleuteld Excel bestand) waren vanuit productieregie op de Q-schijf geplaatst. Die waren daarna ingelezen in SAS. Het output bestand bevat een lijst van BSNs met het resultaat goed. De output is in SAS bewaard. Een backup is ook in een map op de Q-schijf bewaard. Het bestand is toegankelijk voor alle D.A.T. medewerkers.
- Werkopdrachten:** in deze stap worden de posten toegevoegd waarvan we uit de werkopdrachten weten dat ze in toezicht hebben gezeten. Vervolgens worden daar de beschikkingen aan gekoppeld van vóór en na het toezicht. Afhankelijk van het soort toeslag en verschil tussen het bedrag voor en na de controle wordt bepaald of een post als goed of fout wordt geclassificeerd. Deze verwerking gebeurt in SAS. Gegevens uit het data fundamenteel (TVS en beschikkingen) worden gebruikt. Het output bestand bevat een lijst van BSNs met het resultaat goed of fout. De output is in SAS bewaard. Het bestand is toegankelijk voor alle D.A.T. medewerkers (zie Risico's en Maatregelen).
- Intensief toezicht teams:** de Intensief toezicht teams houden een centrale lijst bij van posten die vanwege opzet niet compliant zijn. Een selectie hiervan kan als fout case toegevoegd worden aan het model. Ook deze stroom is lopend, hoewel aantallen relatief beperkt zijn.

³⁹ GreenLane project uit 2016: Verschuiving van integraal toezicht naar onderbouwd selectief toezicht.

De gegevens (In een onversleuteld Excel bestand) worden door de Intensief toezicht team op de Q-schijf geplaatst. Die worden daarna ingelezen in SAS. Het output bestand bevat een lijst van BSNs die in SAS bewaard wordt. Een backup is ook in een map op de Q-schijf bewaard. Het bestand is toegankelijk voor alle D.A.T. medewerkers.

- **DTCheck:** als extra check willen we posten hebben die niet gecontroleerd zijn en die als goed getypeerd kunnen worden. Dit is nu alleen gedaan voor toeslagjaar 2017. Daarbij is gekeken naar het verschil tussen VT⁴⁰ en DT⁴¹ en meldingen die aanvragers hebben gedaan. Uit het bestand wat zo verkregen is, is een gestratificeerde steekproef getrokken zodat de steekproef op een aantal achtergrondkenmerken overeenkomt met de populatie. Deze verwerking gebeurt in SAS. Gegevens uit het data fundament (beschikkingen) worden gebruikt. Het output bestand bevat een lijst van BSNs met het resultaat goed of fout. De output is in SAS bewaard. Het bestand is toegankelijk voor alle D.A.T. medewerkers.

2. Bepalen behandelresultaat (goed / fout)



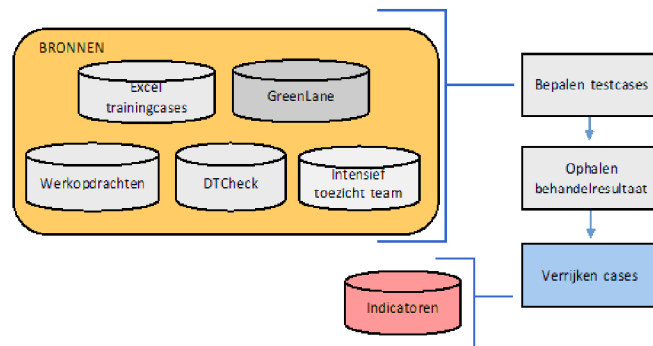
Voor elke bron zijn businessrules opgesteld wanneer een case 'fout' of 'goed' wordt genoemd. Per herkomst is de aanpak hiervan verschillend:

- **Excel:** bij opzet van het model en bij gebrek aan betere trainingcases is ervoor gekozen om een selectie van BSN's die over een langere periode geen mutaties hebben doorgevoerd allemaal als 'Goed' te labelen, ondanks dat hiervoor niet is vastgesteld of de case daadwerkelijk compliant was. Door steeds meer cases te toevoegen wordt de kans kleiner of een oneerlijk samengestelde trainingset.
- **GreenLane:** alle posten die in deze iteraties als compliant beoordeeld zijn, kunnen als 'goed' case toegevoegd worden aan de trainingset.
- **Werkopdrachten:** aan de werkopdrachten worden beschikkingen gekoppeld van vóór en na het toezicht. Afhankelijk van het soort toeslag en verschil tussen het bedrag voor en na de controle wordt bepaald of een post als goed of fout wordt geclassificeerd.
- **Intensief toezicht team:** alle posten die hieronder vallen, worden als 'fout' toegevoegd aan de trainingset.
- **DTCheck:** alle posten die hieronder vallen, worden als 'goed' toegevoegd. Omdat we over weinig goede cases beschikken hebben we voor 2017 goede cases gehaald uit DT-beschikkingen die nauwelijks afwijken van de VT.

3. Verrijken cases

⁴⁰ Voorlopige Toekenning

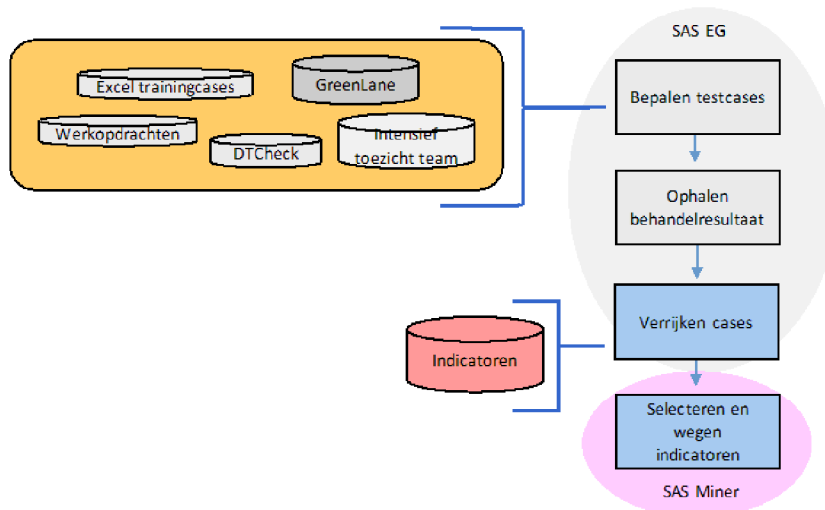
⁴¹ Definitieve Toekenning



Aan de cases voegt een geautoriseerde medewerker van DAT gegevens over de aanvraag en aanvrager toe die pas in de vervolgstap worden geanalyseerd op voorspellende kracht. Dit zijn de indicatoren⁴² die gebruikt worden om het scoremodel te bepalen. De indicatoren worden toegevoegd vanuit verscheidene bronnen (zie bijlage 3 en 4).

Deze gegevens worden gekozen op relevantie voor de toeslagsoort en op basis van heuristieken van medewerkers van DAT, HHR en Toezicht. De resulterende trainingsset en de indicatorenlijst worden opgeslagen in SAS en op de Q-schijf.

4. Selecteren en wegen indicatoren



De verrijkte gegevens worden met statistische-analyse-software SAS Enterprise Miner geanalyseerd op voorspellende kracht waarna hun gewing in de voorspelling wordt bepaald. Door interactive grouping⁴³ wordt elke indicator onderverdeeld in bins, waarna bepaald wordt of de indicator

⁴² De indicatoren zijn tijdens de bouwfase van het model gecreëerd tijdens een brainstormsessies tussen HHR en de behandelaars van het Toezicht team. Die selectie was gebaseerd op huidige en eerdere ervaringen uit het toezichtpraktijk.

⁴³ Zie voor een beschrijving: <https://documentation.sas.com/?docsetId=emre&docsetTarget=p1qzwz7onopjqcn11uc04i18urg7.htm&docsetVersion=15.1&locale=en>

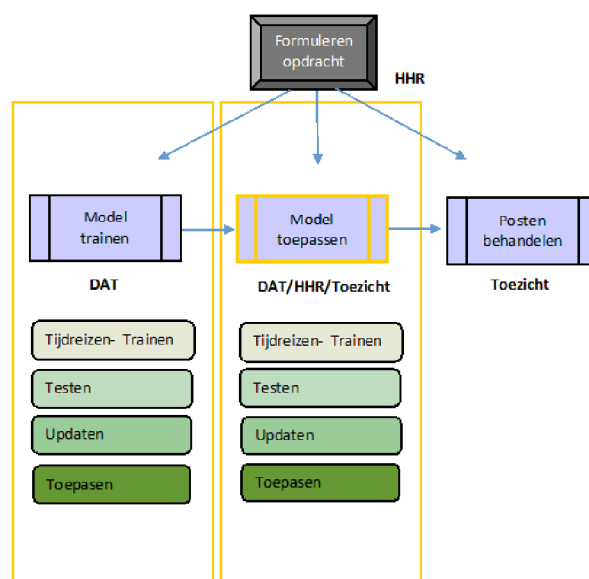
verklarend genoeg is om te voorspellen of een beschikking goed of fout verklaard wordt (volgens de Gini coëfficiënt⁴⁴).

Door middel van een logistische regressiemodel wordt een scorecard⁴⁵ gemaakt, waaruit blijkt hoeveel gewicht elke bin heeft in het voorspellen van goed of fout. De som van de gescoorde indicatoren geeft de eindscore, waarvan een hogere score betekent dat de aanvraag een relatief hogere kans op fout heeft dan een lagere score.

De resulterende scorecard wordt opgeslagen als code in SAS en als een Excel bestand op de Q-schijf.

De scorecard wordt daarna gebruikt om de risicoscore van de aanvragen te bepalen (zie onderdeel B. hieronder voor toepassing van het model).

B. Toepassen van het model

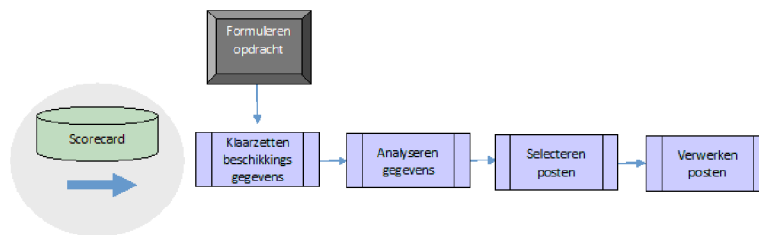


Hoofdproces

⁴⁴ Gini coëfficiënt: ook wel Gini-index, is een statistische maatstaf van de ongelijkheid in een verdeling.

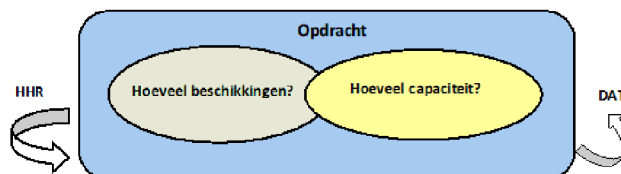
⁴⁵ Zie voor een beschrijving:

<https://documentation.sas.com/?docsetId=emre&docsetTarget=n181vl3wdwn89mn1pfpqm3w6oaz5.htm&docsetVersion=14.3&locale=en>



Proces	Omschrijving	Organisatie
1. Formuleren opdracht	Een intelligence analist van HHR geeft opdracht aan DAT een bepaald aantal toeslagaanvragen te selecteren met de hoogste kans op fout. Een controller van productieregie bepaalt wat de behandelnorm per type post is en een intelligence analist bepaalt hoeveel (afhankelijk van de behandelcapaciteit er beschikbaar is die maand) en waaraan aanvragen moeten voldoen om in aanmerking te komen voor selectie door het model. Een data analist voert de daadwerkelijke selectie uit.	HHR, PR
2. Voorbereiden scorecard	Geautoriseerde medewerkers van DAT bepalen met behandelde posten welke eigenschappen van een aanvraag voorspellend zijn voor het fout zijn van een aanvraagbeschikking, wat resulteert in een scorecard (zie <u>trainen van het model</u>)	DAT
3. Klaarzetten beschikingsgegevens	DAT ontvangt van verschillende bronnen gegevens in een beveiligde omgeving en koppelt deze gegevens aan de beschikkingen	DAT
4. Analyseren gegevens	Geautoriseerde medewerkers van DAT analyseren de beschikkingen aan de hand van gekoppelde gegevens en de scorecard, wat resulteert in gerangschikte beschikkingen	DAT
5. Selecteren posten	Geautoriseerde medewerkers van DAT selecteren te behandelen posten aan de hand van de gerangschikte beschikkingen en behandelcapaciteit. Een Toezicht medewerker voert een steekproef uit op de geselecteerde posten om te controleren of de verwachte risicoscore juist is. Geautoriseerde intelligence analisten van HHR controleren het resultaat en herinitiëren het proces als nodig. Als alle stappen volgens verwachting zijn verlopen, biedt de intelligence analist de gewenste aantallen en welke posten niet meegenomen hoeven te worden aan, aan een data analist.	DAT, Toezicht, HHR
6. Verwerken posten	Geautoriseerde medewerkers van DAT leveren de beschikkingen aan het Toeslagen queryloket. Het queryloket maakt werkopdracht aan waaruit bundels volgen die worden aangeleverd aan CAP-UPG om ingelezen te worden in TVS voordat het formeel beschikken gaat draaien. Als ze in TVS staan, worden ze door Toeslagen werkvoorbereiding aangeboden aan medewerkers van IST om de geselecteerde posten te behandelen	DAT, Toezicht

1. Formuleren opdracht

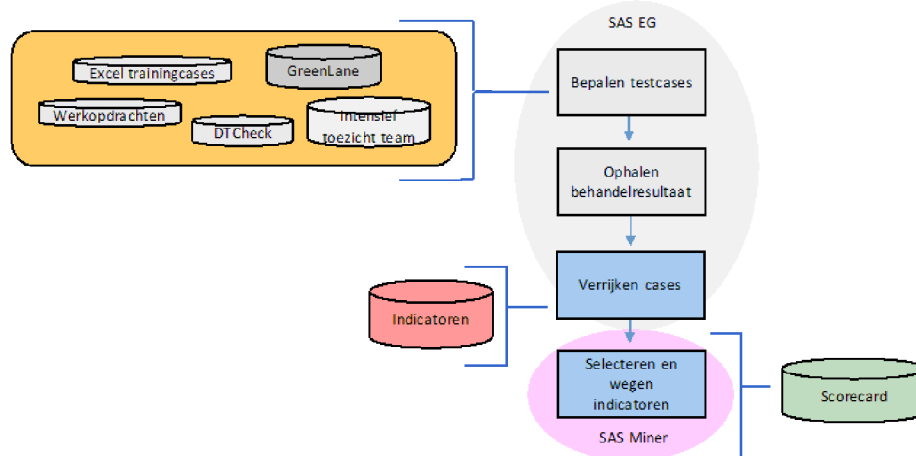


Proces	Omschrijving	Organisatie
1.1 Behoefte aan het classificeren van beschikkingen wordt uitgesproken	HHR bepaalt dat beschikkingen voor huurtoeslag, kinderopvangtoeslag en KGB dienen te worden classificeren.	HHR
1.2 Beschikbare capaciteit wordt bepaald	HHR en PR ⁴⁶ bepalen hoeveel posten hoog risico KOT, hoog risico HT en hot-hor ⁴⁷ aangeboden worden voor handmatige behandeling. Het document waarin dit is vastgelegd wordt gedeeld met DAT per e-mail. Dit document bevat geen persoonsgegevens.	HHR, PR

2. Voorbereiden Scorecard

⁴⁶ Productieregie

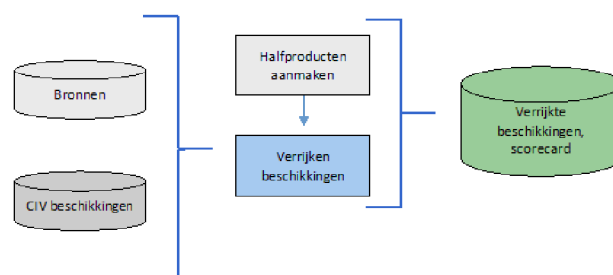
⁴⁷ Hot Hor: hoge teruggaaf/hoog risico



Het proces om de scorecard voor te bereiden is reeds beschreven in sectie A. Het trainen van het model. Het doel van het voorbereiden van de scorecard is het bepalen welke indicatoren⁴⁸ voorspellen of een aanvraag goed of fout gekeurd wordt en hoe zwaar deze indicatoren wegen. Het resultaat is een scorecard met te beoordelen indicatoren en hun weging. Randvoorwaarden voor een betrouwbare scorecard zijn een frequente toevoer van nieuwe testcases en voldoende gegevens over behandelde aanvragen en aanvragers. Hiermee blijft de trainingset aan testcases up-to-date, zodat de scorecard nieuwe types fouten kan blijven vaststellen. Aan de hand van de resulterende scorecard vindt in een vervolgstap de beoordeling plaats van de relatieve kans op het foutief bevinden van nieuwe aanvragen.

Het model wordt sinds een jaar geleden niet meer getraind maar het proces wordt herhaald voor het voorbereiden van de scorecard. Steekproeven worden weinig uitgevoerd vanwege gebrek aan capaciteit.

3. Klaarzetten beschikingsgegevens



Het doel van het klaarzetten van beschikingsgegevens is het verzamelen van gegevens over de aanvraag en aanvrager voor analyse en filtering in vervolgstappen. DAT ontvangt daarvoor ruwe

gegevens van dataleveranciers (zie bijlagen 1) en zet deze om tot koppelbare data. De samenvoeging van deze data, al koppelbare gegevens uit het datafundament en beschikkingen, vormt een grote dataset. De gegevens in deze dataset maken het mogelijk een uitspraak te doen over de relatieve kans op het foutief beoordelen van de aanvraag. Ook kan met deze gegevens in een vervolgstap een filtering plaatsvinden op basis van criteria die HHR stelt.

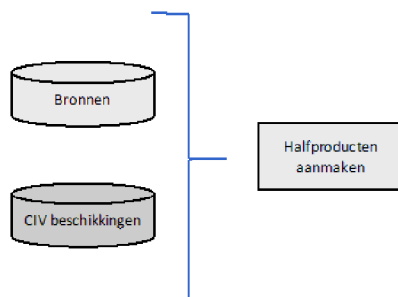
Proces	Omschrijving	Organisatie
3.1 Halfproducten aanmaken	DAT ontvangt van verschillende bronnen (zie bijlage 1) gegevens en bereidt deze voor om te koppelen aan beschikkingen	DAT
3.2 Verrijken beschikkingen	Geautoriseerde medewerkers van DAT koppelen gegevens uit halfproducten en het datafundament aan beschikkingen	DAT

Brondata is afkomstig van diverse afdelingen binnen Toeslagen. De manier waarop deze data aangevraagd en verkregen wordt verschilt per dataset. In alle gevallen is de inhoud van de aanvraag bij de leverende partij bekend (meestal is sprake van gestandaardiseerde queries). De verversing van brondata impliceert in de regel dus enkel een herhaling van bekende zetten. Per run wordt bepaald voor welke bronnen nieuwe data opgevraagd wordt. Voor iedere dataset die verversd moet worden, wordt aan de betreffende contactpersoon per email een nieuwe data-aanvraag gestuurd. Hiervoor wordt een opvraaglijstje bijgehouden.

Gegevens worden vaak per e-mail ontvangen als Excel of csv bestanden (zie bijlage 1 en 2 "ontvangstmethode" bij bronnen en halfproducten).

In veel gevallen vindt levering van de data plaats via een gedeelde netwerkschijf. Gegevens uit CIV worden na het afronden van een officiële aanvraag en een WMK toets door CAP klaargezet in een uitwisselmap op de netwerkschijf. Vervolgens worden deze door een data-analist gekopieerd naar de SAS Grid van Toeslagen, waar alleen data-analisten die belast zijn met de risicoclassificatie bij kunnen. Na ontvangst wordt de brondata direct gecontroleerd op plausibiliteit en bruikbaarheid. Deze controles worden bijgehouden in de risicoclassificatie controlematrix (zie bijlage 5). Bij bevindingen zal overleg plaatsvinden met de leverende partij, deze blijft in principe verantwoordelijk voor de kwaliteit van de data.

3.1 Halfproducten aanmaken



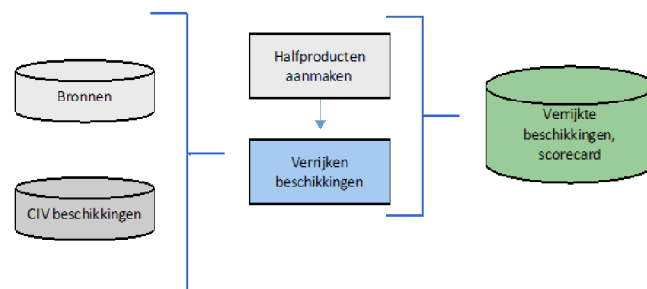
Na ontvangst van nieuwe brondata worden de hiervan afhankelijke halfproducten ververst. Elk halfproduct zet brondata om in een tabel die, vaak op het BSN, aan de (concept)beschikkingen gekoppeld kan worden. Het gaat in de halfproducten voornamelijk om 'contra-informatie': kenmerken van de aanvrager of aanvraag die in de vorm van indicatoren gebruikt worden als input voor het risicoclassificatiemodel.

Alle halfproducten bestaan uit een enkel SAS Enterprise Guide project. In de meeste gevallen zal het betreffende project hiervoor niet of nauwelijks aangepast hoeven te worden, en zal enkel het betreffende project opnieuw gedraaid moeten worden.

De verwerking wordt gecontroleerd op fouten en implausibele resultaten. De resultaten van deze controles worden bijgehouden in de risicoclassificatie controlematrix.

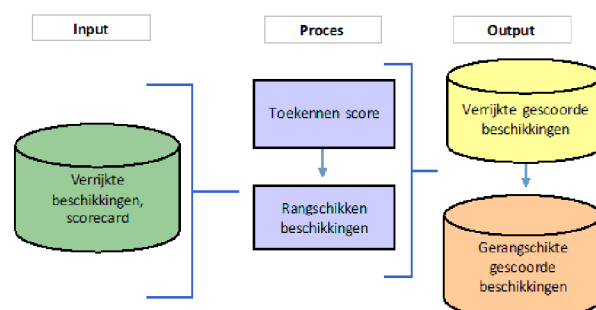
Nadat het proces gedraaid heeft worden de halfproducten in het model (HT_model en KOT_model) aan de beschikkingen gekoppeld.

3.2 Verrijken beschikkingen



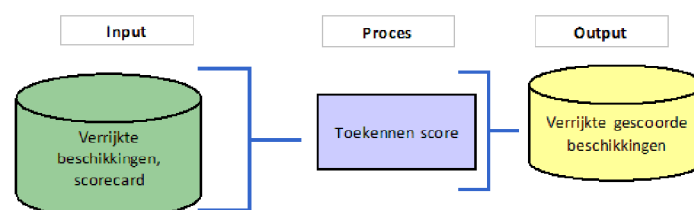
Koppeling van details uit de aanvraag vanuit de (concept)beschikkingen en contra-informatie vanuit de halfproduct. De gegevens uit de halfproducten worden gekoppeld aan de gegevens van de beschikking dataset die op het datafundament staat. Met deze data worden bepalingen gedaan zoals afstand KOO-aanvrager, hoogste maandbedrag, etc.

4. Analyseren Gegevens



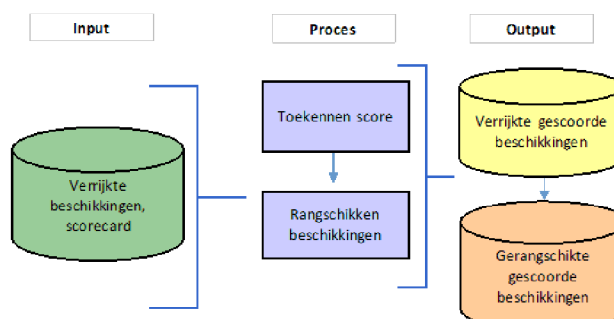
Proces	Omschrijving	Organisatie
4.1 Toekennen score	Geautoriseerde medewerkers van DAT kennen per beschikking een score toe op basis van de scorecard	DAT
4.2 Rangschikken beschikkingen	Geautoriseerde medewerkers van DAT rangschikken gescoorde beschikkingen op hoogste kans van foutief	DAT

4.1 Toekennen score



Toekenning van risicoscores aan alle (concept)beschikkingen aan de hand van het getrainde risicoclassificatiemodel. De output van deze stap is de ruwe output van het model. Voor alle in het model gebruikte indicatoren is het aantal ScoreCard-punten bepaald. De scorecard wordt gebruikt om per BSN elke verklarende variabele een score te geven. De scores van verklarende indicatoren worden bij elkaar opgeteld. De hoogste score is de relatief hoogste kans op een foute aanvraag en vice versa.

4.2 Rangschikken beschikkingen

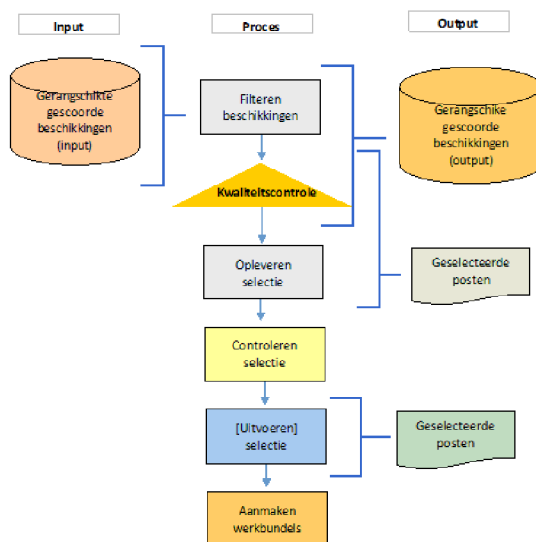


Door rangschikken is het mogelijk een selectie te maken van de groepsaanvragen waar de verwachte hitrate het hoogste is.

Het resultaat wordt als een Excel bestand op de netwerkschijf opgeslagen.

Om te finaliseren worden de gescoorde aanvragen nabewerkt zodat aan elke aanvraag een opvolgactie toebedeeld kan worden, en de diverse vormen van output samengesteld worden.

5. Selecteren Posten

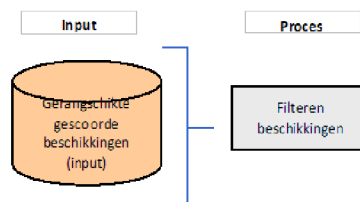


Proces	Omschrijving	Organisatie
5.1 Filteren beschikkingen	Geautoriseerde medewerkers van DAT filteren beschikkingen op basis van criteria waaraan een beschikking moet voldoen om in aanmerking van selectie te komen	DAT
5.2 Kwaliteitscontrole	Het proces zelf en de output worden gecontroleerd aan de hand van de controlematrix	DAT
5.3 Opleveren selectie	Geautoriseerde medewerkers van DAT leveren aan een intelligence analist van HHR een lijst met geselecteerde beschikkingen	DAT, HHR, PR
5.4 Controleren selectie	Een Toezicht medewerker voert een steekproef uit op de geselecteerde posten om te controleren of de verwachte risicoscore juist is, geautoriseerde intelligence analisten van HHR controleren het resultaat en koppelt terug als een aanpassing gewenst is.	Toezicht, HHR, PR
5.5 Uitvoeren selectie	Geautoriseerde medewerkers van DAT leveren een definitieve selectie van beschikkingen aan een intelligence analist van HHR en stuurt de geselecteerde posten aan TQL ⁴⁹ om te verwerken	DAT, HHR, TQL
5.6 Aanmaken	TQL zorgt ervoor dat werkbundels worden	TQL

⁴⁹ Toeslagen Query Loket

werkbundels	aangemaakt	
-------------	------------	--

5.1 Filteren beschikkingen – (opvolgacties)



Behalve de risicoscore zijn er nog een aantal kenmerken van de aanvraag of aanvrager die bepalen wat er met de conceptbeschikking gebeurt. Deze stap is ook nodig om te bepalen of een aanvraag onderdeel van de risicoselectie is of niet en om de juiste behandeling aan de burger te geven:

- Is de toeslagaanvraag 'op nul gezet'?
- Is voor het BSN van de aanvrager recent een bezwaar afgehandeld?
- Is de aanvrager een 'onbekende aanvrager'?
- Wordt de betreffende BSN voor de betreffende regeling al uitgesloten van beschikken (staat BSN op de 'uitsluitlijst') of was dit recent het geval?
- Is sprake van geen recht op toeslag vanwege 'bijvangst'?
- Is de laatste beschikking een conceptbeschikking?
- Is de aanvraag nieuw of leidt een mutatie tot een hogere toeslag dan voorheen?
- Vormt de aanvraag vanwege een hoog bedrag een hoog risico ('Hot Hor' – alleen voor KOT)?
- Is er een overledene bij de aanvraag betrokken?

Deze kenmerken worden per toeslagaanvraag in het model vastgesteld. Vervolgens wordt aan de hand van deze kenmerken per aanvraag bepaald wat de relevante opvolgactie is. De volgende opvolgacties zijn mogelijk:

- Geen Actie
- Op uitsluitlijst vanwege onbekende aanvrager
- Op uitsluitlijst vanwege Hot Hor (alleen KOT)
- Op uitsluitlijst vanwege bijvangst
- Op uitsluitlijst vanwege hoog risico

Op nul gezet

'Op_nul_gezet' is een indicator die aangeeft of de aanvraag een actuele conceptbeschikking met een jaarbedrag van 0 euro is (1=Ja, 0=Nee). De bepaling van deze indicator vindt plaats in DTM_HT en DTM_KOT.

Als de aanvraag op nul gezet is, dan is de afgeleide conclusie dat het gaat om een aanvraag die door een toeslagmedewerker behandeld is, waarbij de conclusie is doorgevoerd dat geen sprake is van een rechtmatige aanvraag.

Om te voorkomen dat een aanvraag die op nul gezet is, vervolgens door de risicoclassificatie uitgesloten wordt van beschikken, volgt op deze aanvragen nooit een uitsluiting en is de actie altijd 'Geen Actie'.

Recent afgehandeld bezwaar

Het halfproduct 'bezwaren' geeft een lijst van BSN's waarvoor recent (sinds de vorige run van formeel beschikken van het betreffende Toeslagjaar) door Toeslagen een bezwaar is afgehandeld. De kans is groot dat een conceptbeschikking voor een BSN met een afgehandeld bezwaar een consequentie is van deze afhandeling (dit kan zowel toekenning als afwijzing van het bezwaar zijn). Om te voorkomen dat in die situatie de conceptbeschikking uitgesloten wordt, volgt in het geval van een recent afgehandeld bezwaar nooit de actie 'uitsluitlijst'.

Onbekende aanvrager

Voor de zorgtoeslag worden handmatige controles uitgevoerd op het zorgverzekerd zijn van burgers. Om risicogericht toezicht uit te voeren wil directie Toeslagen voor aanvragers zorgtoeslag weten of zij wel recht hebben op deze toeslag.

Onbekende aanvragers zijn burgers die woonachtig zijn op een Nederlands adres maar zijn uitgesloten voor formeel beschikken omdat zij de status onbekende aanvragers hebben.

Een onbekende aanvrager is een aanvrager:

- met een BSN dat jonger is dan 1 jaar;
- waarvoor geen enkele toeslagregeling een formele beschikking met een jaarbedrag groter dan 0 euro is uitgereikt;
- na de vorige risicoclassificatierun een nieuwe conceptbeschikking is ontstaan.

Deze aanvragers worden in het algemeen beschouwd als een hoog risico, omdat ze bij Toeslagen relatief onbekend zijn. Aanvragen van onbekende aanvragers worden daarom in beginsel uitgesloten van beschikken. De onbekende aanvragers worden hierop uitgenodigd op een Belastingkantoor om bewijsstukken (bijv. huurcontract of overeenkomst met kinderopvanginstelling) te overleggen.

Bijvangst

Bijvangst zijn toeslagaanvragen waarvoor op basis van harde criteria (op basis van de Awir) vastgesteld kan worden dat in geen geval sprake zal zijn van recht op toeslag.

Voor HT zijn deze criteria:

- Voor de BSN is in de BVR geen adres bekend (Vertrokken Onbekend Waarheen - VOW) of
- de aanvraag heeft betrekking op een adres dat is uitgesloten voor huurtoeslag (vastgesteld obv halfproduct 'uitgesloten adres')

Voor KOT zijn deze criteria:

- De aanvrager woont niet in Nederland, België of Duitsland of
- Een kind waarvoor KOT wordt aangevraagd woont niet in Nederland, België of Duitsland of
- De leeftijd van het oudste kind waarvoor KOT wordt aangevraagd is hoger dan 15.

Omdat bij bijvangst geen sprake kan zijn van recht op toeslag wordt de betreffende aanvraag in principe uitgesloten.

Uitzonderingen zijn:

- Er is een overledene bij de aanvraag betrokken. Om pijnlijke situaties te voorkomen wordt in dat geval niet uitgesloten.
- Er is een recent afgehandeld bezwaar voor de aanvrager.
- De beschikking is geen concept – in dat geval valt er niets uit te sluiten.
- Het betreft geen nieuwe aanvraag en geen mutatie met een hoger bedrag dan voorheen.

Uitsluitlijst

De uitsluitlijst is een lijst van BSN's die voor een bepaalde toeslagregeling en voor een bepaald tijdvak uitgesloten worden van beschikken. De risicoclassificatieruns leveren input voor deze uitsluitlijst, maar de uitsluitingen kunnen ook uit andere onderdelen van de organisatie komen.

In het proces worden historische uitsluitingen gebruikt om te voorkomen dat iemand die op het moment van selectie uitgesloten is, of dat recent was, voor een tweede keer of nogmaals uitgesloten wordt. Per run wordt echter inhoudelijk getoetst of die vertaling passend is.

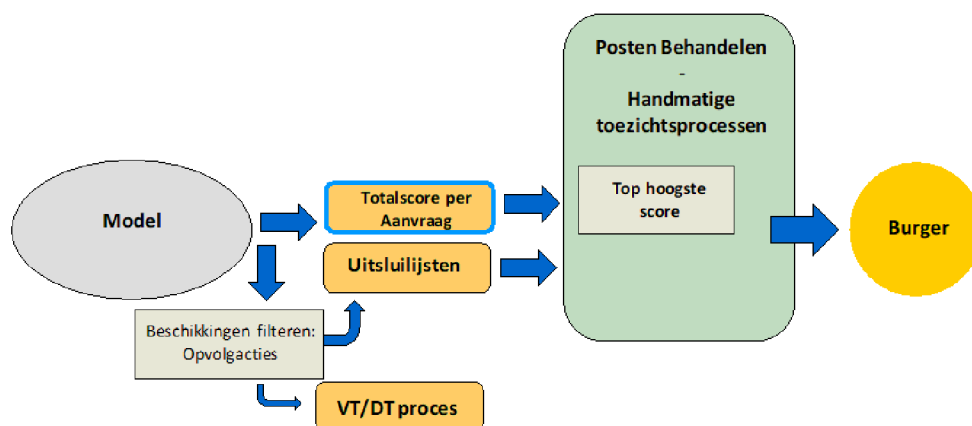
Een belangrijke aanname is dat iemand die recent uitgesloten is en op het moment van selectie niet meer, door Toeslagen behandeld en daarom vrijgegeven is. Na een dergelijke vrijgave is het niet de bedoeling dat de conceptbeschikking alsnog uitgesloten en geblokkeerd wordt. Alle BSN's die recent zijn uitgesloten van beschikken, worden daarom niet opnieuw uitgesloten.

In theorie is het mogelijk dat na een afvoering van de BSN van de uitsluitlijst, de aanvrager een mutatie opgeeft die leidt tot een nieuwe conceptbeschikking. Die mutatie wordt door de risicoclassificatie vanwege bovenstaande implementatie niet op risico geselecteerd. Omdat bij zowel de opvoering als afvoering van een BSN niet geregistreerd wordt wat de reden voor opvoering dan wel afvoering was, en bij de generatie van een conceptbeschikking niet bekend is of de beschikking een gevolg is van een handeling van de aanvrager of een medewerker van Toeslagen, kan hier in het proces geen rekening mee gehouden worden.

HOT-HOR:

De posten hoog risico KOT, hoog risico HT en HOT-HOR worden aangeboden voor handmatige behandeling. Dit zijn actuele conceptbeschikkingen met een hoog bedrag (dus een hoog risico). Deze stap heeft ook als doel het beschermen van de burger zodat geen hoge terugvorderingen worden ontvangen.

De outputbestanden (uitsluitlijsten) worden gebruikt binnen het handmatig administratief Toezicht proces. De mogelijke risico's die kunnen ontstaan door deze lijsten is al geanalyseerd in de GEB M861 Behandelen Fraudesignalen.

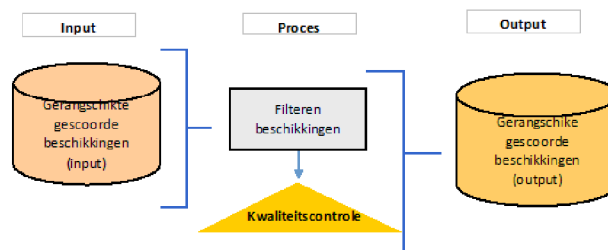


Als resultaat van het filteren van beschikkingen zijn de volgende acties mogelijk:

- Een aanvraag wordt gemarkeerd als uitworp (uitsluitlijst) wanneer op grond van de risicogerichte beslisregels/kenmerken twijfel bestaat over de rechtmatigheid. Dat betekent dat nadere handmatige controle van de berekende toeslag is nodig. Dit proces wordt verder gedetailleerd in GEB Handmatige behandeling van onvolledige en/of tegenstrijdige toeslagenaanvragen (Uitval/uitworp) M2077.

- Een aanvraag wordt binnen het VT /DT⁵⁰ proces behandeld (dit is een geautomatiseerd proces; zie verder GEB Definitief Toekenning Toeslag M675 en Automatisch continueren (MAC) toeslag M1647)

5.2 Kwaliteitscontrole



Nadat het model gedraaid is wordt de inputdata, het proces zelf en de output gecontroleerd aan de hand van de controlematrix. Pas nadat alle controles afgerond zijn, worden de diverse vormen van output met de rest van de organisatie gedeeld.

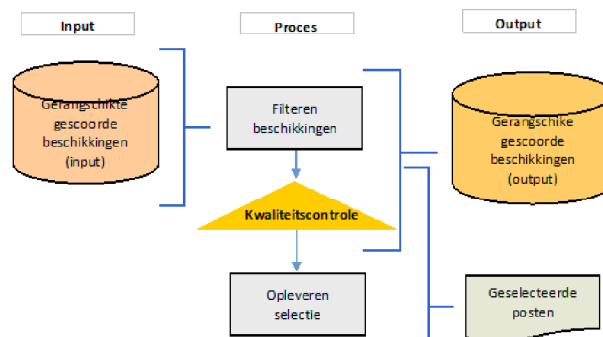
Om de kans op fouten tijdens een risicoclassificatierun zo klein mogelijk te maken is een controlematrix samengesteld (zie bijlage 5).

De matrix geeft een lijst met handmatig uit te voeren checks. Deze checks zijn open geformuleerd, er is in de meeste gevallen geen sprake van een norm of gekwantificeerd criterium waaraan voldaan moet zijn. Dit legt de verantwoordelijkheid voor de invulling van de controles bij de controleurs neer. Deze controleurs zullen dus vanuit hun expertise moeten beoordelen of aan de benodigde voorwaarden voldaan moet worden.

De controles voor tijdreizen en de modellen (HT en KOT) worden in principe onder een vierogenprincipe uitgevoerd om fouten te voorkomen die grote gevolgen voor de kwaliteit van het model kunnen hebben. De andere controles worden uitgevoerd door de collega (DAT) die het betreffende proces tijdens de risicoclassificatierun behandelt.

5.3 Opleveren selectie

⁵⁰ Voorlopige Toekenning / definitief Toekenning



De definitieve run resulteert in verschillende vormen van output:

- Een inhoudelijke uitsluitlijst ('met reden'), die gebruikt wordt om aan de uitsluiting opvolging te geven (bijvoorbeeld in communicatie met de betreffende burger). De reden geeft aan op welke grond de post is geselecteerd.
- Een overzichtstabel, waarin de aantallen posten over een aantal categorieën gegeven worden getoond. Deze tabel vormt de basis voor een rapportage over de resultaten van de risicoclassificatierun.
- Voor KOT: een lijst met alle Hot Hor posten die echt behandeld gaan worden.
- Een eindbestand waarin per BSN alle risicoscores zitten.

De bestanden worden in SAS bewaard en in csv formaat op de Q-schijf als back-up opgeslagen.

De resultaten van een run worden per e-mail opgeleverd naar de postbus van QueryLoket, Werkvoorbereiding en Kantoorregisseurs.

In de e-mail worden de volgende bestanden opgeleverd in csv formaat:

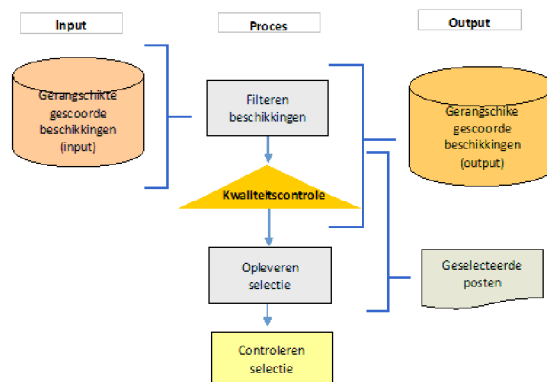
- De uitsluitlijsten (één per regeling KOT en HT)
- De overzichtstabel
- De lijst met alle Hot Hor posten

Deze bestanden heeft het Queryloket nodig om de posten uit te sluiten en Productie Regie om werkbundels aan te maken.

De manier hoe de bestanden worden opgeleverd zal in Q2 2021 worden aangepast volgens de nieuwe richtlijnen voor veilig uitleveren van AU⁵¹ (zie Risico 8 en 9 in Hoofdstuk 16 en 17 Risico's en Maatregelen)

5.4 Controleren selectie

⁵¹ Analytics United



Iedere maand worden Hoog Risico posten uitgezet ter controle. Deze posten worden geselecteerd op basis van beschikbare toezichtcapaciteit en de risicoscore. Om de selectie te valideren wordt vóór het definitief selecteren van de posten, steekproeflijsten opgesteld door HHR en uitgezet bij de Toezicht teams. Vanuit de selectie worden meerdere lijsten/acties gedraaid, deze worden gecontroleerd door HHR & Toezicht.

Proefrun en definitieve run

Voor het draaien van de proefrun bespreken de data en intelligence analisten met elkaar welke aantallen er opgeleverd gaan worden. Bij de proefrun wordt er een aantal Excel lijsten uitgezet ter controle bij het Toezicht team. Als de ingevulde Excel lijsten terug gestuurd worden bereken HHR aan de hand van de hoog risico-lijsten het percentage posten dat door de steekproevers als risicovol wordt gezien.

- ✓ Er wordt met kwaliteitsregie afgestemd of er een kwaliteitscheck is gedaan.
- ✓ Het percentage risicovol per regeling wordt uitgerekend. De uitkomsten en redenen worden afgestemd met de data-analisten en er wordt een beslissing over de selectie bij de definitieve run genomen.
- ✓ De uitkomsten van het verslag worden besproken met de data-analisten en gedocumenteerd.

De steekproef heeft verschillende doeleinden. Het is een check om te beoordelen of een toeslagaanvraag terecht door het risicoclassificatiemodel als risicovol is aangemerkt. De behandelaar controleert of de aangeboden BSN's daadwerkelijk risicovol zijn. Dit doet hij o.b.v. enkele factoren (bijv. voor KOT: hoge opvanguren, verhouding inkomen - aantal opvanguren - kosten en voor Huur: verhouding inkomen - huurprijs, ronde huurprijzen, hoge servicekosten, evt. oppervlakte woning en aantal personen op de beschikking). Dit is belangrijk want het model selecteert de posten voor Risicoclassificatie en impliciet dus ook waar wij toezicht op inzetten, de controle door de behandelaar zorgt er voor dat die kan bevestigen of het model de juiste/risicovolle aanvragen eruit haalt. Daarnaast worden de resultaten van de steekproef gebruikt om de verdeling tussen Hoog Risico HUUR, Hoog Risico KOT en HOT-HOR te bepalen. Het kan namelijk voorkomen dat in de ene maand de Hoog Risico HUUR risicovoller is dan Hoog Risico KOT, met tot gevolg dat er naar verhouding meer HUUR uitgezet wordt.

Onderdeel van de steekproef is de validatiecheck, waar wordt gekeken naar het percentage van de posten die terecht als hoog risico geselecteerd zijn. Deze validatiecheck wordt door een van de behandelaars van het Toezicht team per e-mail naar HHR en DAT gestuurd. Zie voorbeeld:

Categorie	Dimensie	Aantal
Steekproef	Percentage van steekproef terecht geselecteerd als hoog risico	98
Steekproef	Posten uit populatie getrokken in steekproef	49

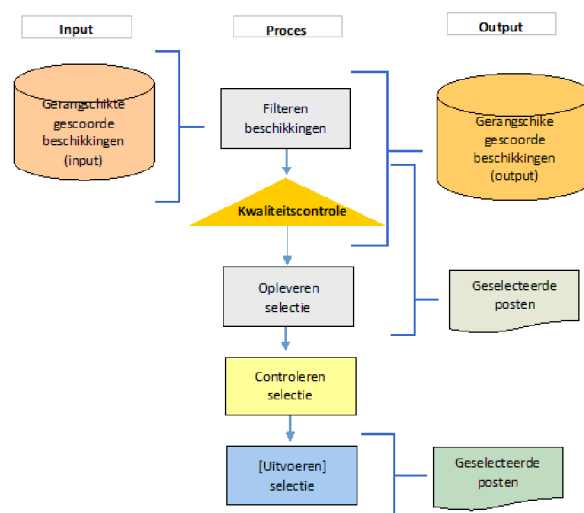
Als onderdeel van het validatieproces wordt naar de 'hitrates' gekeken: het percentage posten wat gecorrigeerd is na behandeling.

Naast hitrate wordt er een statistische toets op accuratesse gedaan (gini-score: als die te laag is, is het model te weinig verklarend).

De combinatie van de hierboven benoemde technieken biedt extra betrouwbaarheid omdat het niet alleen de verklarende waarde van je model bekijkt, maar ook de werking in de praktijk. Een model kan heel goed verklarend zijn maar niets opleveren.

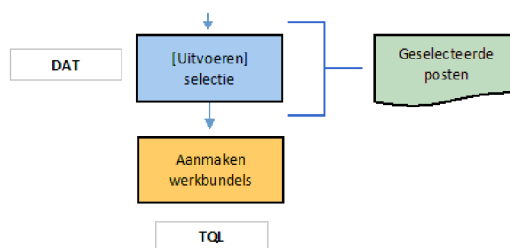
Momenteel wordt de proefrun op de dag van de definitieve run uitgevoerd. Een verandering ten opzichte van de runs van voor november 2019 is dat er geen maandelijkse steekproef wordt uitgevoerd op de nieuwe aanvragen/mutatie Hoog Risico KOT en HUUR. Deze steekproef wordt enkel uitgevoerd als het model getraind wordt. Redenen die hebben geleid tot aanpassingen in steekproeven zijn o.a. de afnemende toezichtcapaciteit, risicogerichte keuzes, dat steekproeven veel tijd vergen en dat HHR meer kan met de beschikbare data.

5.5 Uitvoeren selectie



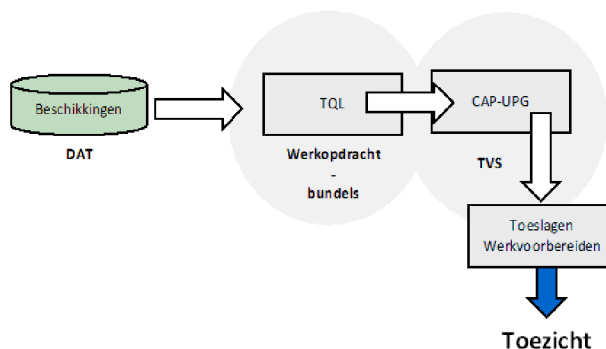
Na de validatie van de selectie levert DAT na een definitieve run een definitieve selectie van beschikkingen aan HHR. De geselecteerde posten worden per e-mail naar de postbus van TQL verstuurd om te verwerken.

5.6 Aanmaken werkbundels



TQL zorgt ervoor dat werkbundels worden aangemaakt zodat behandelaars de posten verder kunnen controleren.

6. Verwerken posten



DAT levert de beschikkingen (geselecteerde posten) aan het Toeslagen queryloket. Het queryloket maakt werkopdracht aan waaruit bundels volgen die worden aangeleverd aan CAP-UPG om ingelezen te worden in TVS voordat het formeel beschikken gaat draaien. Als ze in TVS staan, worden ze door Toeslagen werkvoorbereiding aangeboden aan medewerkers van Toezicht om de geselecteerde posten te behandelen.

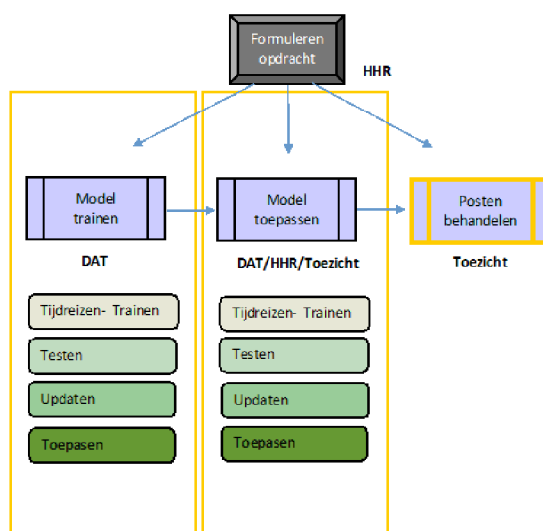
Werkwijze:

Werkbundels worden ontvangen middels een serviceaanvraag en begeleidende mail. Door de beperkte hoeveelheid bijlagen die ITSM aan kan worden deze ook via de mail aangeleverd. De serviceaanvragen zijn voor iedereen inzichtelijk die aan groep BCA12002 (=CAPHeffing Toeslagen Functioneel Beheer) is gekoppeld. De bijlagen in de postbus zijn voor iedereen toegankelijk die rechten heeft tot de postbus 'CAP Toeslagen Productie_Postbus'.

De werkbundels worden verwerkt conform de instructies in het opdrachtformulier. De bestanden worden vanuit de mail of serviceaanvraag verplaatst naar een directory op de Q-schijf. Vanuit het Kantoorportaal wordt de opdracht gestart om de bestanden te verwerken. Alle leden van de vakgroepen 'Formeel Beschikken' en 'Productie Coördinatoren' hebben het recht om deze bestanden via het Kantoorportaal te verwerken. Na verwerking wordt de verwerkte werkbundel in een archiefmap op de Q-schijf geplaatst. Middels een query op de toeslagendatabase wordt bij een ongelijk aantal tussen aangeleverde en verwerkte items het verschil verklaard en teruggekoppeld aan Kantoor. Daar wordt vervolgens bepaald of er een nieuwe werkbundel aangeleverd wordt.

Het resultaat van de verwerkingen is het uitsluiten voor het formeel beschikken. Die wordt gedeeld via een reactie op de serviceaanvraag en op de gestuurde mail.

C. Het behandelen van de posten



Het Toezicht team controleert als behandelaar de geselecteerde posten. Behandelaars kunnen contact opnemen met de burger om informatie aan te vragen en soms wordt informatie aan externe partijen zoals de KOO of de verhuurders gevraagd. Soms is het met een check op de contra-informatie voldoende om te bepalen of een wijziging nodig is en of de aanvraag rechtmatig of onrechtmatig is.

Dit proces wordt hier niet verder geanalyseerd omdat het binnen de scope valt van GEB M8776 Toezicht. De mogelijke risico's zijn wel meegenomen in hoofdstuk 16.

Beveiliging – Autorisatiebeleid

Uit paragraaf 3.2.3.4 van het iBB: De Belastingdienst hanteert een generiek beveiligingsniveau dat voor informatiebeveiliging overeenkomt met BBN2 van de BIO. De BIO (Baseline Informatiebeveiliging Overheid) vormt hiervoor het gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen). Dit niveau is gericht op de beveiliging van verwerking van persoons- en financieel economische gegevens (departementaal vertrouwelijk volgens het VIRBI⁵²), inclusief het aspect privacy. De maatregelen voor fysieke beveiliging en voor personele veiligheid en integriteit sluiten hierop aan, dat wil zeggen, ondersteunen het generieke beveiligingsniveau. Dit betekent dat alle bedrijfsmiddelen beschermd worden op het niveau van BBN2, ook als er minder bescherming nodig is. Een uitzondering hierop kan alleen gemaakt worden indien de verwerking

⁵² Voorschrift Informatiebeveiliging Rijksdienst.

buiten de Belastingdienst plaatsvindt en door middel van een risicoanalyse is aangetoond dat een lager beveiligingsniveau aanvaardbaar is. Aanvullende maatregelen bovenop het generieke worden genomen op basis van een risicoanalyse. Een risicoanalyse is verplicht in de volgende gevallen:

- BIV hoger dan midden-midden-midden voor gegeven of proces;
- Dreiging komt niet voor in het dreigingsprofiel;
- Bekende onvolkomenheden in de implementatie van het generieke beveiligingsniveau.

De verantwoordelijkheid voor risicoanalyse, mitigatie en acceptatie ligt bij de directie die het risico draagt. Van interne en externe leveranciers (dienstverleners) wordt geëist dat actief op beveiligingsrisico's wordt gestuurd en worden gerapporteerd aan de risicodragende directie.

Autorisatiebeleid

In de autorisatiematrix IMS worden bedrijfsrollen aangemaakt. Aangewezen medewerkers krijgen deze bedrijfsrollen toegekend door de direct leidinggevende ter ondersteuning van de uitvoering van opgedragen werkzaamheden. Controle op uitgegeven bedrijfsrollen gebeurt via het LTB proces (logisch toegangsbeheer). Conform de BIO moeten alle teamleiders minstens 2x per jaar de autorisaties controleren. Centraal is door SSO F&MI in IMS geregeld dat als een medewerker doorstroomt naar een ander dienstonderdeel de autorisaties van het latende dienstonderdeel na 14 dagen automatisch worden ingetrokken.

Analyseomgeving: datafundament, SAS EG, SAS Miner

De analyseomgeving waar de directie Toeslagen gebruik van maakt, wordt inclusief toegangsmanagement geleverd door het domein Analytics. IV GBS (voorheen IV Accent) is verantwoordelijk voor het beheer van de analytics omgeving. Dit komt nog uit de Investeringsagenda. Toen was besloten dat het beheer van de Analytics omgeving los van de reguliere IV werd ingericht. En het Domein Analytics is verantwoordelijk voor de kaders omtrent analytics resulterende in de Domein Architectuur Analytics. Dat doen zij in samenwerking met de diverse analytics afdelingen, zoals DF&A, Toeslagen analytics, Douane analytics, IV COE Analytics, etc. Het domein bestaat maar uit 2 personen. Het werk wordt gedaan door de deelnemers uit de aangesloten analytics afdelingen.

Autorisaties verlopen via IMS en worden toegekend door van het team Data Analytics Toeslagen (DAT) binnen directie Toeslagen. De medewerker Informatiebeveiliging binnen directie Toeslagen valideert vervolgens de autorisatie aanvraag. Op het moment van schrijven, 17 november 2020, hebben in totaal 13 medewerkers toegang tot het datagebied voor het risicoclassificatiemodel, het betreft 9 analisten en 4 beheerders/ontwikkelaars van het fundament. Afhankelijk van de opdracht kunnen deze medewerkers gegevens raadplegen, koppelen aan andere gegevens en gebruiken voor verdere analyse, waarbij de instructies uit de opdracht gevolgd worden. De gegevens worden geautomatiseerd door het domein Gegevens in de analyseomgeving geladen, of via een handmatig proces door de beheerders van directie Toeslagen, zijnde medewerkers van DAT.

Ondanks het autorisatiebeleid is de toegang tot de gegevens in SAS m.b.t. het RCM niet voldoende beperkt. Op dit moment is er geen specifieke groep medewerkers die als enige geautoriseerd zijn om te werken aan het RCM model. Dit is ook de situatie op de netwerkschijf. Een accurate toewijzing van autorisaties en logging ontbreekt deels waardoor mutatie- en exportrechten ten onrechte gebruikt zouden kunnen worden. (zie Risico's en Maatregelen)

Voor verdere informatie over de inrichting van het datafundament, aanvragen van datagebieden en technische en organisatorische maatregelen, zoals pseudonimisering en gebruikte richtlijnen en kwaliteitsprocessen, verwijzen wij naar de GEB M8778 Datafundament. Zie ook bijlage 7 voor een overzicht van de interne processen.

Logging en monitoring in het kader van Informatiebeveiliging

De Minister van Financiën, voor deze d[] Belastingdienst, voor deze de algemeen [] is verantwoordelijk voor het loggen en monitoren van het gebruik van de ICT-infrastructuur (verwerking M2854). Doel hiervan is het uitvoeren van het geldende beveiligingsbeleid en oplossen van problemen door het analyseren van (oneigenlijk) gebruik van ICT infrastructuur. Het gaat om de logging van het BSN en IP-adres van burgers, met datum/tijd en uitgevoerde actie, en het IP-adres en user ID van medewerkers⁵³, met datum/tijd en uitgevoerde actie. Dit heeft betrekking op alle ICT-systemen van de Belastingdienst en directie Toeslagen en de uitvoering hiervan ligt bij het Security Operation Center (SOC) van de Belastingdienst.

Specifiek voor het datafundament is er monitoring op een aantal vooraf gedefinieerde handelingen. Als een van deze handelingen zich voordoet dan wordt de Business Security Officer van Toeslagen hierover geïnformeerd die een beoordeling doet en een mogelijk vervolgonderzoek instelt. De monitoring ziet toe op:

- specifieke zoekopdracht naar 1 burger
- specifieke zoekopdracht naar bankrekeningnummer
- exporteren van gegevens

(Semi) geautomatiseerde besluitvorming

Er is sprake van semi-geautomatiseerde besluitvorming. Aan de hand van het RCM wordt bepaald of een aanvraag hoog risico is. Afhankelijk van de behandelcapaciteit worden de posten met de hoogste risico in behandeling genomen door de behandelteams van Toeslagen. Door gebruik te maken van semi-geautomatiseerde besluitvorming is het mogelijk om voor Toeslagen op een efficiënte wijze de posten met de hoogste risico's te selecteren.

Met het risicoclassificatiemodel vindt echter geen uitsluitend geautomatiseerde besluitvorming plaats, aangezien aanvragen met een hoog risico worden aangeboden voor handmatige beoordeling door een medewerker van Toeslagen. (AP "Onderzoek Belastingdienst Kinderopvangtoeslag")

Het gebruik van het risicoclassificatiemodel door Toeslagen is een vorm van profileren omdat deze verwerking voldoet aan alle drie de voorwaarden genoemd in artikel 4, aanhef en onder 4, van de AVG. Ten eerste is sprake van een geautomatiseerde vorm van verwerking. Het risicoclassificatiemodel is namelijk een algoritme dat automatisch aanvragen selecteert waarop personele capaciteit wordt ingezet. Ten tweede heeft de verwerking betrekking op persoonsgegevens. De informatie die gebruikt wordt voor de indicatoren in het risicoclassificatiemodel zijn persoonsgegevens als bedoeld in artikel 4, aanhef en onder 1, van de AVG. Ten derde heeft de verwerking met het risicoclassificatiemodel ten doel om individuele kenmerken te evalueren en categoriseren. Aan de hand van persoonlijke aspecten van de aanvrager wordt geëvalueerd en op basis daarvan ingeschat hoe groot het risico is dat de aanvrager een onjuiste aanvraag heeft ingediend, en wordt het toezicht daarop afgestemd.

Profileren, waarop geen uitsluitend geautomatiseerde besluitvorming is gebaseerd, is op grond van artikel 22 van de AVG toegestaan. Het is een verwerking waarvoor, net als voor alle andere verwerkingen, een grondslag aanwezig moet zijn en waarvoor de overige waarborgen van de AVG gelden. (AP "Onderzoek Belastingdienst Kinderopvangtoeslag")

Art. 22 Avg bevat het recht voor betrokkenen om niet onderworpen te worden aan besluiten die op uitsluitend geautomatiseerde verwerking gebaseerd zijn. Dit recht in verband met geautomatiseerde besluitvorming komt in feite neer op een verbod voor dergelijke besluiten. Dit verbod is echter

⁵³ Zie bijlage met OR instemmingverzoek monitoring.

zeker niet absoluut. Hierbij is als eerste van belang om vast te stellen of er sprake is van een uitzondering op het verbod van art. 22, lid 1, AVG. Hierbij speelt art. 40, lid 2, UAvG een rol. Op grond van art. 40, lid 2, UAvG dienen maatregelen genomen te worden die strekken tot bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. In het geval van het risicoclassificatiemodel is de menselijke tussenkomst een maatregel om eventueel ongerechtvaardigd of ongewenst onderscheid dat toch door het geautomatiseerde risicoclassificatiemodel mogelijk gemaakt kan worden, te beoordelen en zo nodig te 'repareren'. Daarom is het risicoclassificatiemodel gebaseerd op semi-geautomatiseerde besluitvorming.

9. Juridisch en beleidsmatig kader



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

Algemene wet inkomensafhankelijke regelingen (AWIR): artikel 11. Directie Toeslagen voert de inkomensafhankelijke regelingen uit die haar zijn opgedragen, te weten: de Zorg-, Huur en kinderopvangtoeslag en het Kindgebonden budget. Directie Toeslagen is belast met het toekennen, uitbetalen en terugvorderen van tegemoetkomingen. Op grond van deze wetgeving kan dus worden gesteld dat directie Toeslagen is belast met de publiekrechtelijke taak om uitvoering te geven aan het toekennen, uitbetalen en terugvorderen van ZT, HT, KOT en KGB. Bij de uitvoering van deze taken moet de directie Toeslagen de procedure volgen die is vastgelegd in hoofdstuk 2, paragraaf 2 Awir. Dat betekent o.a. dat directie Toeslagen in het lopende jaar voorschotten verleent (artikel 16 Awir en definitieve toekenningen (art. 19, Awir, na afloop jaar).

Daarnaast past de gegevensverwerking in het vastgestelde beleid van directie Toeslagen. Dit blijkt bijvoorbeeld uit de handhavingsvisie en het Klantsegment Toeslagen waarin behandeling op maat alsmede informatiegericht risicodetectie ten doel zijn gesteld. Verdere informatie over de beleidsmatige uitwerking van de doelen staat beschreven in het Toeslagen Toezicht Werkplan 2018.

Bij de controle van ingediende aanvragen en bij de toekenning wordt gebruik gemaakt van de gegevens waarover de directie Toeslagen reeds beschikt. Zo beschikt de directie Toeslagen reeds over de inkomensgegevens en gegevens over de huishoudsituatie. Voor de huurgegevens bestaat in het kader van de uitvoering van de Huursubsidiewet reeds een automatische uitwisseling van huurgegevens met een aantal verhuurders (deels woningcorporaties). Op basis van deze gegevens kan een effectieve controle van de huurgegevens plaatsvinden. De controlemogelijkheden die deze automatische uitwisseling van huurgegevens met zich meebrengt, blijft ook in de toekomst, als de uitvoering van de huursubsidie in handen van de directie Toeslagen komt, gewenst (Uit de MVT Awir).

Als een voorschot is verleend, is de aanvrager verplicht bepaalde wijzigingen door te geven (artikel 17 Awir jo. artikel 5 Uitvoeringsregeling Awir). Daarnaast is een aanvrager, partner of medebewoner (gegevens van medebewoners worden alleen voor huurtoeslag verwerkt) verplicht mogelijk relevante gegevens en inlichtingen te verstrekken, als directie Toeslagen daarom vraagt (art. 18 Awir).

De hoogte van de kinderopvangtoeslag is onder andere afhankelijk van de draagkracht van de aanvrager en de eventuele toeslagpartner. Hiervoor wordt het toetsingsinkomen in aanmerking genomen (artikel 7, eerste lid, Awir, en artikel 1.7, eerste lid onderdeel a, Wko). Daarnaast is de hoogte afhankelijk van de kosten van kinderopvang, waaronder het aantal uren afgenomen kinderopvang (artikel 1.7, eerste lid onderdeel b, Wko). Om die reden dienen relevante wijzigingen in deze omstandigheden binnen vier weken door aan de directie Toeslagen te worden doorgegeven

(artikel 5 Uitvoeringsregeling Awir). Als deze wijzigingen echter niet (tijdig) worden doorgegeven, dan kan er een te hoog voorschot zijn verleend, dat door de directie Toeslagen moet worden teruggevorderd (artikel 26 Awir).

Publiekrechtelijke organisaties, zoals DUO en UWV, en aangewezen andere personen en organisaties zijn verplicht om gegevens en inlichtingen aan directie Toeslagen te verstrekken waarvan de kennisneming van belang kan zijn voor de uitvoering van de Awir (artikel 38, eerste lid, Awir). In artikel 1a, eerste lid, onderdeel b, van het Uitvoeringsbesluit Awir zijn de kinderopvangorganisaties aangewezen voor de levering van de gegevens, bedoeld in artikel 11, eerste lid, onderdeel b, van de Regeling Wko.

Daarnaast verstrekken inspecteur en ontvanger aan de directie Toeslagen gegevens en inlichtingen uit die nodig zijn voor de uitvoering van de Awir (artikel 39, eerste lid, Awir).

Door middel van Horizontaal Toezicht ontvangen wij van externe organisatie gegevens.

Om de dienstverlening voortvloeiend uit de uitvoering van de Awir te verbeteren, willen de hiervoor genoemde contractspartijen gaan samenwerken. De grondslag voor deze samenwerking is gelegen in artikel 38a van de Awir en het Uitvoeringsbesluit Algemene wet inkomensafhankelijke regelingen (Staatsblad 2005, 431, laatstelijk gewijzigd Staatsblad 2014, 579, hierna: Uitvoeringsbesluit). Dit is het geval bij COA-Vluchtelingenwerk.

Voor deze wettelijk verplichting waaraan externe organisatie gebonden zijn, geldt dat zij persoonsgegevens verwerken als verwerkingsverantwoordelijke.

Uitwerking van de normen inzake verwerking van het BSN:

De memorie van toelichting van artikel 46 van de UAVG luidt als volgt: *Dit artikel voorziet in een algemene regeling voor gebruik van identificatienummers, waaronder als belangrijkste het burgerservicenummer (BSN). Vanwege de extra risico's die het gebruik van dergelijk nummers met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, wordt in het onderhavige artikel daarenboven bepaald dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de desbetreffende wet (verdere verwerking) alleen mogelijk is voor zover dat bij de wet is bepaald.*

De memorie van toelichting van de Wabb zegt over het gebruik van het BSN onder meer het volgende:

De kern van deze actualisering bestaat uit de introductie van het burgerservicenummer (BSN) voor de klantcontacten tussen burger en overheid waarbij het gebruik van een persoonsnummer nodig is ten behoeve van eenduidige identificatie en registratie van personen en voor de gegevensuitwisseling tussen overheidsorganisaties onderling. Het wetsvoorstel regelt dat alle overheidsorganen het nummer mogen gebruiken bij het verwerken van persoonsgegevens in het kader van hun publieke taak, zonder dat daarvoor nadere regelgeving vereist is. Voor het gebruik buiten de kring van overheidsorganen blijft een specifieke wettelijke grondslag nodig. Het wetsvoorstel reguleert niet de gegevensverwerkingen in het kader waarvan het burgerservicenummer als hulpmiddel wordt gebruikt. Die gegevensverwerkingen dienen aan de daarop betrekking hebbende eisen, zoals onder meer vastgelegd in de Wbp, te voldoen. Het wetsvoorstel geeft voor wat betreft het gebruik van het burgerservicenummer slechts de grondslag voor overheidsorganen om het burgerservicenummer bij zo'n elders gereguleerde gegevensverwerking te gebruiken. Met het onderhavige wetsvoorstel wordt beoogd om een sluitend stelsel van persoonsnummers te realiseren. Met het woord sluitend wordt bedoeld dat het stelsel zodanig is ontworpen dat de persoonsnummers de hulpmiddelen vormen waarvoor ze bedoeld zijn, namelijk om het beheer van persoonsgegevens in diverse administraties en registraties te vereenvoudigen. Daarnaast mogen in een sluitend stelsel geen oneigenlijke rollen aan persoonsnummers worden gehecht. Persoonsnummers moeten alleen gebruikt worden wanneer dat nodig is. Als een overheidsorgaan een dienst kan leveren zonder dat het nodig is om gegevens van de persoon vast te leggen of te raadplegen, dan is het niet nodig om een persoonsnummer bij deze

transactie te betrekken. Het gebruik van het burgerservicenummer kent een aantal verschijningsvormen. In de eerste plaats dient het burgerservicenummer voor opname in een registratie van een organisatie, zodat de gegevens van een persoon doeltreffend zijn terug te vinden. In de tweede plaats is het burgerservicenummer een hulpmiddel bij het ophalen of raadplegen van algemene persoonsgegevens zoals die in de GBA en de toekomstige registratie van niet-ingezetenen zijn vastgelegd. In de derde plaats is het burgerservicenummer een hulpmiddel bij het raadplegen van gegevens die in andere registraties zijn opgeslagen, bijvoorbeeld op het gebied van inkomens of opgebouwde verzekeringsrechten. In de context van een registratie waarin persoonsgegevens worden opgeslagen, is het burgerservicenummer een hulpmiddel om gegevens goed te kunnen opslaan, te bewerken en terug te zoeken. Aangezien het burgerservicenummer geen informatie bevat, is het niet mogelijk om er informatie aan te ontleen die de persoonlijke levenssfeer kan raken. Het burgerservicenummer is daarmee te beschouwen als een administratief hulpmiddel waarvan het toegestane gebruik in een registratie samenvalt met het toegestaan zijn van de registratie zelf. Teneinde overheidsorganen de mogelijkheid te bieden in het kader van de uitvoering van hun publiekrechtelijke taken bij het verwerken van persoonsgegevens waar mogelijk gebruik te maken van het burgerservicenummer, is in het onderhavige artikel [10 Wabb] een algemene bevoegdheid daartoe opgenomen.

10. Bewaartermijnen



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

Klik hier om infotekst te verborgen

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering: indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij conceptregelgeving zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij overheidsverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.

Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder
------	--	--	---	-----------------------

Elk overheidsorgaan is zelf verantwoordelijk voor het opstellen van een selectielijst die voldoet aan de wettelijke eisen. Hiervoor geldt een zorgvuldige procedure omdat er verschillende belangen zijn: van de bedrijfsvoering van uw organisatie, van recht- en bewijszoekenden en van historische onderzoekers.

Op grond van artikel 12, tweede lid, Regeling Archiefbeheer Belastingdienst 2011 (RAB 2011) is voor directie Toeslagen een selectielijst vastgesteld en gepubliceerd in Stcrt. 2015/31399 (zie ook artikel 5 van de Archiefwet 1995).

Het archiefbeherend onderdeel draagt zorg voor de vernietiging van de daarvoor in aanmerking komende archiefwaardige informatieobjecten na het verstrijken van in de selectielijst daarvoor vastgestelde termijn. Bij fysieke informatieobjecten gebeurt dit door Doc-Direct (zie artikel 16, eerste lid, RAB 2011). Bij digitale informatieobjecten gebeurt dit vanuit de Toeslagen Archiefvoorziening (TAV). Van de te vernietigen archiefwaardige informatieobjecten wordt een verklaring van vernietiging opgesteld. Deze wordt ondertekend door B/CFD, unit Documenthuishouding (zie artikel 16, tweede lid, RAB 2011).

De bewaartermijn voor producten die voortkomen uit het verzamelen, analyseren en veredelen van gegevens en deze omzetten in relevante handavingsinformatie (intelligenceproces) bedraagt op grond van de Selectielijst Toeslagen 7 jaar na vervallen.

Het betreft hier producten (in- en output) zoals: Interne/ externe uitvoeringsgegevens, fraude- en risicosignalen, verkenningen, (evaluatie)onderzoeken, werkbundels, contra-informatie. Dit betreft producten uit processen A en B.

De bewaartermijn voor producten die voortkomen uit het nemen van besluiten over het te kiezen handavingsinstrumentarium bedraagt op grond van de Selectielijst Toeslagen 7 jaar na vervallen. Het betreft hier producten (in- en output) zoals: kaders, advies, (concept) convenanten, handavingsplannen, intelligenceopdrachten, werkbundels/werkvoorbereiding, effect- en mismatchrapportages, uitsluitlijsten. Dit betreft producten uit proces C.

In de Awir staat niet expliciet een bewaartermijn bepaald, maar volgens jurisprudentie geldt een bewaarplicht van vijf jaar. Zie ABRvS 1 juni 2016, ECLI:NL:RVS:2016:1484.

De in de selectielijst opgenomen termijnen zullen hun achtergrond hebben in dat de Awir en jurisprudentie herhaaldelijk een termijn van vijf jaar nadat het berekeningsjaar is verstreken, noemen (zie bijvoorbeeld artikel 21, tweede lid, Awir, en zie bovengenoemde uitspraak ABRvS). Bijvoorbeeld: 2015 'verjaart' per 1 januari 2021. Stukken die betrekking hebben op 2015, hebben we in beginsel dus niet meer nodig na 6 jaar. Met die 7 jaar hebben we een extra marge ingebouwd (en deze is ook conform de 'blauwe' bewaartermijn), zodat we niet te vroeg vernietigen. Er kan immers tegen het eind van de verjaringstermijn (in het voorbeeld uiterlijk op 31 december 2020) nog een herzieningsverzoek binnenkomen, waarmee we iets moeten doen. Als de stukken dan al

vernietigd zouden zijn, hadden wij we geen stukken om het verzoek te kunnen beoordelen. Vaak geldt zelfs een termijn van 12 jaar, omdat de toeslag bij een wijziging in verband met het inkomensgegeven altijd herzien moet worden (artikel 20 Awir). Er geldt dan in feite een verjaringstermijn die in de AWR wordt gehanteerd: op grond van de AWR kan een inkomensgegeven bij vermogen in het buitenland zelfs nog tot 12 jaar na het belastingjaar worden gewijzigd.

Binnen Toeslagen wordt er naast reguliere applicaties ook gebruik gemaakt van gegevens in de vorm van lijsten en extracten. Deze gegevens worden door medewerkers op de persoonlijke omgeving, de e-mail of op samenwerkingsgebieden op de netwerkschijf bewaard. Hierbij blijft zorgvuldigheid van belang om onterecht gebruik, datalekken of onbedoelde vernietiging te voorkomen.

Ingevolge artikel 5 lid 1 sub e AVG mogen persoonsgegevens niet langer worden bewaard dan voor de doeleinden noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, mits passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen. Momenteel is er geen formeel proces voor het vernietigen van gegevens in SAS en op de Q-schijf. Dit is echter belangrijk om te kunnen voldoen aan de bewaartermijn van de selectielijst. In Q2 2021 zullen er stappen genomen worden richting het vernietigen van de gegevens in SAS en de Q-schijf, om het risico van opslagbeperking te voorkomen (zie risico 9 in hoofdstuk 16 en 17 Risico's en Maatregelen). Tijdens deze implementatie zal ook geëvalueerd worden of een back-up van de output en de tussenbestanden van het risicoclassificatiemodel op de Q-schijf moet blijven worden opgeslagen. De reden daarvoor zou zijn dat SAS Grid een applicatie is van een derde partij en wij ons er van willen verzekeren dat wij kunnen voldoen aan inzageverzoeken, audits en uitlegbaarheid. Momenteel zijn back-up bestanden alleen via SAS toegankelijk voor geautoriseerde medewerkers van DAT.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

- b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het

kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

In Hoofdstuk 2, paragraaf 5 van de Awir (artikelen 38 t/m 39a) is de informatieverstrekking aan en de informatie-uitwisseling door directie Toeslagen geregeld.

Artikel 38, over de informatieverstrekking aan directie Toeslagen, is er ook verder uitgewerkt in het uitvoeringsbesluit Awir (de artikelen 1a en 1b). Het laatste artikel bepaalt dat de gegevens worden verstrekt aan directie Toeslagen onder vermelding van het BSN.

In de artikelsgewijze toelichting op artikel 38 Awir staat o.a. het volgende: Dit artikel regelt de kosteloze verstrekking aan de directie Toeslagen van gegevens en inlichtingen waarvan de kennisneming van belang kan zijn voor de uitvoering van deze wet. Omdat, afhankelijk van de regeling waarop dit wetsvoorstel van toepassing is, de aanspraak op of de hoogte van een tegemoetkoming mede afhankelijk kan zijn van informatie die niet binnen de rijksbelastingdienst of de directie Toeslagen voorhanden is, is in het eerste lid voor decentrale overheden, bepaalde semi-overheidslichamen en voor bij algemene maatregel van bestuur aangewezen natuurlijke personen, maat- en vennootschappen, verenigingen en andere rechtspersonen, instellingen en diensten een verplichting tot informatieverstrekking opgenomen. Het gaat dan vanzelfsprekend om gegevens en inlichtingen waarover die betrokken persoon of instantie redelijkerwijs geacht wordt te beschikken.

Publiekrechtelijke organisaties, zoals DUO en UWV, en ieder ander die bij AMvB is aangewezen zijn desgevraagd verplicht om gegevens en inlichtingen aan directie Toeslagen te verstrekken waarvan de kennisneming van belang kan zijn voor de uitvoering van de Awir (art. 38, eerste lid, Awir): *(Openbare lichamen met uitzondering van de openbare lichamen Bonaire, Sint Eustatius en Saba en rechtspersonen die bij of krachtens een bijzondere wet rechtspersoonlijkheid hebben verkregen, de onder hen ressorterende instellingen en diensten, lichamen die hoofdzakelijk uitvoering geven aan het beleid van het Rijk, administratieplichtigen als bedoeld in [artikel 52 van de Algemene wet inzake rijksbelastingen](#) en verhuurders van een woning als bedoeld in [artikel 1, onderdeel k, van de Wet op de huurtoeslag](#) verstrekken kosteloos aan de Directie Toeslagen desgevraagd alle gegevens en inlichtingen die van belang kunnen zijn voor de uitvoering van deze wet, de daarop berustende bepalingen of een inkomensafhankelijke regeling.)*

Zo worden in art. 1a, eerste lid, van het Uitvoeringsbesluit Awir onder meer de kinderopvangorganisaties, verhuurders en zorgverzekeraars genoemd. Zij zijn verplicht om bepaalde informatie desgevraagd aan directie Toeslagen te verstrekken. Voor de kinderopvangorganisaties betreft het de gegevens, bedoeld in art. 11, eerste lid, onderdeel b, van de Regeling Wko.

De Informatieverplichting van het eerste lid van artikel 38 Awir treedt in werking op het moment dat de Directie Toeslagen de gegevens en inlichtingen opvraagt bij de betreffende partij. In beginsel kan aan alle voornoemde lichamen, instellingen, diensten, rechtspersonen of personen alle gegevens en inlichtingen worden opgevraagd die van belang kunnen zijn voor de uitvoering van de Awir, de daarop berustende bepalingen of een inkomensafhankelijke regeling (de regelingen die zijn opgenomen in de Wet op de huurtoeslag, de Wet op de zorgtoeslag, de Wet kinderopvang en de Wet op het kindgebonden budget).

Art. 38 Awir is per 1-1-2021 gewijzigd, met inachtneming van overgangsrecht met betrekking tot de berekeningsjaren die vóór 1 januari 2021 aanvangen. De informatieverzoeken die zijn of worden opgelegd op grond van huidige regelgeving met betrekking tot de berekeningsjaren die vóór 1-1-2021 aanvangen blijven dus van toepassing en zullen onveranderd worden gehandhaafd door de Directie Toeslagen.

Verskil tussen het oude en nieuwe art. 38 Awir betreft met name dat lid 1 nu (expliciet) gaat over desgevraagde informatieverstrekking; hieraan zijn, naast 'openbare lichamen', administratieplichtigen en verhuurders van een woning als informatieverstrekkers toegevoegd. Lid 2 gaat over het verplicht 'eigen beweging' verstrekken van informatie. Bedoeling was dit in de UB Awir verder uit te werken (met als belangrijk punt het verplicht maandelijks leveren van informatie door KOO's); dit aangepaste UB is echter nog niet in werking, jongste nieuws is dat de Kamer in de voorhangprocedure heeft aangegeven de basis in de wet zelf te willen i.p.v. in de UB en dat MinFin nu kijkt hoe deze aanpassing van de Awir te regelen (zodat deze hopelijk kan ingaan per 1-1-2022). Daarmee is nog niet duidelijk wat tot dat ingangsmoment te doen met de gegevenslevering.

Doel van wijziging van de Awir op dit punt is, door meer contra-info binnen te halen, om belanghebbende te ontlasten en om terugvorderingen te voorkomen, en om effectiever aanvragen te beoordelen. Dit betekent dat directie Toeslagen kan kiezen of zij (eerst) belanghebbende of de derde benadert; hier is geen rangorde beoogd. De derde kan bij onrechtmatige uitvraag wel kostenvergoeding vragen.

Als uit deze contra-informatie of anderszins blijkt dat het voorschot of de definitieve vaststelling ten onrechte of tot een te hoog bedrag is verleend kan directie Toeslagen het voorschot of de definitieve vaststelling herzien tot het juiste bedrag (art. 16, vijfde lid Awir, respectievelijk art. 21, eerste lid, Awir).

Voor de algemene persoonsgegevens geldt dat de rechtsgrond gebaseerd is op artikel 6, eerste lid, onderdeel e, AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

In artikel 11, tweede lid, van de Awir is immers bepaald dat de directie Toeslagen het organisatiedeel van de rijksbelastingdienst is dat is belast met het toekennen, uitbetalen en terugvorderen van de tegemoetkomingen. In artikel 1.3, eerste lid, van de Wko is dit nog eens expliciet herhaald ten aanzien van de kinderopvangtoeslag.

Publieke taak Artikel 1.3, eerste lid, van de Wko bepaalt dat Toeslagen is belast met de uitvoering van het toekennen, uitbetalen en terugvorderen van de kinderopvangtoeslag. Op grond van het tweede lid van die bepaling is op de Wko de Awir van toepassing. Ingevolge artikel 43 van de Awir, gelezen in samenhang met artikel 1 van het Besluit aanwijzing toezichthouders Awir, is Toeslagen eveneens belast met het toezicht op de naleving van het bepaalde bij of krachtens de Awir. Gelet op de in paragraaf 3.1.2 beschreven positie van Toeslagen, als onderdeel van de onder de minister ressorterende rijksbelastingdienst, kunnen deze taken voor de toepassing van de AVG worden toegerekend aan de minister.

De hoogte van de toeslagen is afhankelijk van de draagkracht van diverse grondslagen, waaronder de draagkracht van de aanvrager, de eventuele toeslagpartner en – bij de huurtoeslag- de eventuele medebewoner. Hiervoor wordt het toetsingsinkomen in aanmerking genomen (art. 7, eerste lid, Awir; art. 1.7, eerste lid onderdeel a, Wko; art. 7 eerste lid, Wet op de huurtoeslag; art. 1, tweede lid, Wet op het kindgebonden budget en art. 1, tweede lid, Wet op de zorgtoeslag).

Daarnaast is de hoogte van de kinderopvangtoeslag afhankelijk van de betaalde kosten van kinderopvang, waaronder het aantal uren afgenomen kinderopvang (art. 1.7, eerste lid onderdeel b, Wko). Voor de huurtoeslag is de hoogte ook afhankelijk van onder andere de rekenuur (art. 21, eerste lid wet op de huurtoeslag).

12. Bijzondere persoonsgegevens



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

[Klik hier om infotekst te verbergen](#)

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

- a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
- b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
- c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
- i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
- j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

- a. wettelijk is toegestaan;
- b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
- c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij conceptregelgeving kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

De overige verwerkte gegevens en de context bij de verwerking van Nederlanderschap door het risicoclassificatiemodel geven geen aanleiding om een indirect verband tussen nationaliteit en ras of etnische afkomst aan te nemen. Het is in dit geval geen sprake van bijzondere persoonsgegevens in de zin van artikel 9, eerste lid, van de AVG. Ook heeft het gebruik niet tot doel om onderscheid te maken naar ras of etnische afkomst.

Nederlanderschap wordt niet meer als indicator in het model gebruikt. De gegevens Nederlanderschap ja/nee die nog onderdeel zijn van de datapreparatie zullen in Q2 2021 verwijderd worden uit het model.

Het gebruik van de BSN nummer:

Directie Toeslagen mag het BSN op grond van artikel 10 van de Wabb gebruiken voor het uitvoeren van zijn taken. Maar dit geldt alleen voor het gebruik waarvoor het BSN is bedoeld, namelijk in de communicatie met de burger en als hulpmiddel voor het registreren en uitwisselen van gegevens.

In de meeste bronbestanden zijn de gegevens gekoppeld aan het BSN en zijn die gegevens per definitie tot personen herleidbaar. Tegelijkertijd is het BSN bedoeld om gegevens/bestanden betrouwbaar te kunnen koppelen. Zonder een betrouwbare koppeling van gegevens is het vrijwel onmogelijk om tot een nauwkeurige risicoselectie te komen. Het niet verkrijgen van een nauwkeurige output kan negatieve gevolgen hebben voor de burgers die onjuist geselecteerd zijn. Deze burgers zouden langer moeten wachten tot hun aanvraag handmatig is goedgekeurd. Voor het versleutelen van het BSN in de bronbestanden en de trainingcases is niet gekozen met als reden dat, gezien de omvang van het team dat toegang heeft tot de gegevens, dit een onevenredige inspanning zou zijn. Daar komt bij dat de bronbestanden los van het BSN ook tot personen herleidbare gegevens kunnen bevatten.

Supervised learning is alleen mogelijk met specifieke cases en dus niet met geaggregeerde gegevens. Voor het leren van het model worden dus de bronbestanden gekoppeld aan de BSN's van de trainingcases. Het BSN van een aanvraag wordt pas in de trainingsset opgenomen nadat een behandelaar de aanvraag heeft onderzocht en een beslissing heeft genomen. Er is dus altijd een menselijke tussenkomst voordat een aanvraag/beschikking als trainingcase wordt opgenomen. In het kader van extra beveiliging wordt, als onderdeel van de maatregelen die gepland zijn voor 2021 (zie Risico's en Maatregelen), de mogelijkheid voor pseudonimisatie en het trainen van het model zonder BSN's te gebruiken onderzocht.

13. Doelbinding



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

de persoonsgegevens oorspronkelijk zijn verzameld.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

- a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
- c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- e. het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

- a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

We gebruiken de gegevens om toeslagen toe te kennen en dat moet rechtmatig gebeuren. De kerntaak van directie Toeslagen is het rechtmatig, juist en tijdig toekennen van de toeslagen. Burgers verstrekken hun gegevens voor het aanvragen (of aanpassen c.q. stopzetten) van een toeslag. De in hoofdstuk 5 genoemde instanties en organisaties verstrekken gegevens voor het kunnen toetsen van de door de burgers verstrekte gegevens (contra-informatie). De oorspronkelijk verzamelde gegevens worden verwerkt voor dit hoofddoel. De verwerking "Risicoclassificatiemodel" is in overeenstemming met dit doel en is direct gekoppeld daaraan.

De directie Toeslagen beoogt met 'handhaving' het gedrag van burgers en bedrijven zodanig te beïnvloeden dat zij structureel (fiscale) regels naleven (compliance). Dit moet zorgen voor de borging van de continuïteit van belastingopbrengsten en de rechtmatige betaling van toeslagen. De directie Toeslagen handelt bij het handhaven binnen de juridische kaders van de wet en conform de beginselen van behoorlijk bestuur.

14. Noodzaak en evenredigheid



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

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

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenoemen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenoemen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.

Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden

met gebruikmaking van een combinatie van gewone persoonsgegevens?

- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

Het in artikel 6, eerste lid, aanhef en onder e, van de AVG neergelegde noodzakelijkheidsvereiste houdt in dat moet worden voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van de persoonsgegevens betrokken personen niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Op grond van het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokken persoon, minder nadelige wijze kunnen worden verwezenlijkt. In het advies 06/2014 van de Groep gegevensbescherming artikel 29 (het huidige Europees Comité voor gegevensbescherming) staat dat de concrete toets is of minder inbreuk makende middelen beschikbaar zijn voor het bereiken van hetzelfde doel.

Om de inbreuk op de persoonlijke levenssfeer van de burgers te beperken zijn maatregelen geïmplementeerd zoals het uitvoeren van steekproeven om de nauwkeurigheid van het model te valideren en het gebruik van semi-geautomatiseerd besluitvorming met menselijk tussenkomst. Een andere mogelijke vorm van rechtsbescherming voor de burger is de mogelijkheid om een klacht/bezwaar bij directie Toeslagen in te dienen.

Proces	Proportionaliteit	Subsidiariteit
A. Trainen van het model	Ons doel als uitvoeringsorganisatie is om juist, tijdig en rechtmatig toeslagen uit te keren. Om met de beperkte middelen die we hebben zo efficiënt mogelijk om te gaan, is het RCM ontwikkeld om zo gericht mogelijk ons toezicht in te zetten. Om dit model te laten functioneren wordt er gebruik gemaakt van een set gegevens die niet elke keer volledig worden gebruikt. Per geval heb je niet altijd de volledige gegevensset nodig. Dit weet je echter pas nadat het model alle gegevens heeft gewogen vandaar dat je	Andere oplossingen om rechtmatig toeslagen toe te kennen zouden de volgende kunnen zijn:
B. Toepassen van het model + opvolgacties		- Steekproefsgewijs controleren: maar dan worden ook burgers geraakt die veel minder risicovol zijn. - Niks te doen vooraf en pas achteraf te controleren als we meer contra-informatie hebben om te gebruiken:

	gegevens niet vooraf uit kunt sluiten. De reden daarvoor is dat het model inspeelt op risicopatronen uit eerdere casussen wat veroorzaakt dat de combinatie van gegevens altijd anders is. Als we van te voren gegevens uit zouden sluiten, zou de risicoscore niet meer zuiver zijn. Het is belangrijk dat het model goed werkt om de juistheid te waarborgen, wat belangrijk is voor het uitvoeren van onze wettelijke taak. De output van het model wordt altijd door een behandelaar gecheckt; op die manier wordt het risico voor de burger verminderd. Het filteren van beschikkingen en het bepalen van opvolgacties nav bepaalde kenmerken is nodig om te bepalen of een aanvraag onderdeel van de risicoselectie is en om de juiste behandeling aan de burger te geven. De reden om een BSN op "Beheer uitsluitingen" in TVS te zetten is om er zorg voor te dragen dat een burger een juiste beschikking krijgt en deze beschikking te controleren voordat deze wordt afgegeven en een onterechte terugvordering te voorkomen. Door een BSN op "Beheer uitsluitingen" te zetten wordt de wijziging van de burger wel in TVS verwerkt en komt er een 'actuele berekening' klaar te staan, maar deze zal niet beschikt worden. Een reeds lopende toeslag wordt hiermee niet gewijzigd, ook niet in de uitbetaling. Dit gebeurt pas nadat dit gecontroleerd is door een medewerker. Deze verwerkingsdoeleinden kunnen een negatieve impact op de persoonlijke levenssfeer van een burger hebben. Het proces voldoet niet aan het beginsel van proportionaliteit. (zie hoofdstuk 16. Risico's en hoofdstuk 17. Maatregelen) Directie Toeslagen beschikt noodzakelijkerwijs over veel gegevens, deze gegevens worden beveiligd. Daarnaast hebben de medewerkers van directie Toeslagen een geheimhoudingsverplichting. Het vastleggen van eerder genoemde gegevens is daardoor geen disproportionele inbreuk op de persoonlijke levenssfeer.	maar dan kunnen burgers achteraf met hoge terugvorderingen worden geconfronteerd. Vanuit uitvoeringsoogpunt is het niet haalbaar om alle aanvragen apart te behandelen en dan dus alleen de gegevens te verwerken die nodig zijn. Om toch zoveel mogelijk aanvragen in de toezichtbehandeling mee te nemen, helpt het om in te schatten welke aanvragen het meest risicovol zijn. Daarbij helpt het Risicoclassificatiemodel. Uitsluitlijsten: Deze verwerkingen kunnen op een andere manier die minder ingrijpend is uitgevoerd worden. Daarom wordt dit proces herijkt. Zie GEB M861 Behandelen Fraudesignalen.
--	---	--

	Hierdoor wordt voldaan aan de beginselen van proportionaliteit.	
A. Posten handmatig behandelen	Om het rechtmatigheidsonderzoek uit te voeren zijn de persoonsgegevens noodzakelijk die betrekking hebben op het vaststellen van het recht op de toeslagen. Hiervoor wordt aan de hand van de in de Awir en desbetreffende toeslagregeling gestelde criteria het recht op de toeslag bepaald. De persoonsgegevens worden gedeeltelijk bij derden uitgevraagd om zo de gegevens ontvangen van de aanvrager te kunnen verifiëren (contra-informatie). Alleen de informatie die nodig is om het recht op, en de hoogte van de toeslag te kunnen vaststellen wordt gevraagd/verwerkt. In dit geval staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de burger in evenredige verhouding tot de verwerkingsdoeleinden. In het geval van posten die onjuist als onrechtmatig zijn aangemerkt wordt de burger onnodig belemmerd. In dit geval kan het bijvoorbeeld langer duren voordat de toekenning definitief beschikt wordt. (Zie Risico 3)	Zonder het vastleggen van deze gegevens kan directie Toeslagen niet vaststellen of er recht is en wat de hoogte van het recht is. Het is niet mogelijk deze vaststelling handmatig op een andere manier te doen. De gegevens, die wettelijk gebruikt worden, worden bij de bron (bijvoorbeeld de inspecteur) opgevraagd. Een alternatief om mensen stelselmatig te bevragen gegevens aan te leveren. Dit is ingrijpender voor burgers en door de omvangrijke populatie niet werkbaar voor directie Toeslagen. Burgers geven niet altijd een juiste voorstelling van de daadwerkelijke situatie. Hierdoor is het noodzakelijk deze gegevens bij andere instanties en organisaties uit te vragen. Directie Toeslagen voldoet daardoor aan de beginselen van subsidiariteit.

15. Rechten van de betrokkene



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

[Klik hier om infotekst te verbergen](#)

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt

aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregulering.

Indien in **conceptregulering** een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregulering genoemde gronden én moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

- a. de verwerkingsdoelstellingen;
- b. de categorieën van persoonsgegevens;
- c. het toepassingsgebied van de ingevoerde beperkingen;
- d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
- e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
- f. de opslagperiodes en de toepasselijke waarborgen;
- g. de risico's voor de rechten en vrijheden van betrokkenen;
- h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

Betrokkenen zijn de natuurlijke personen waarvan de persoonsgegevens worden verwerkt. Dit zijn de aanvragers van de kinderopvang en huurtoeslag, de eventuele toeslagpartner, medebewoners en de kinderen waarvoor kinderopvangtoeslag wordt verstrekt.

De rechten van betrokkenen moeten goed gewaarborgd worden. De directie Toeslagen kent een geheimhoudingsplicht (artikel 2:5 Algemene wet bestuursrecht). Daarnaast worden betrokkenen op internet geïnformeerd over de wijze waarop de directie Toeslagen uitvoering geeft aan de AVG (zie (https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/niet_in_enig_menu/priv/privacy)).

"De doelen waarvoor de Belastingdienst gegevens verwerkt vloeien voort uit de wettelijke taken: heffen, uitkeren, innen, uitoefenen van goederentoezicht en opsporing van delicten die met al deze zaken samenhangen. We gebruiken de voor deze doelen verzamelde gegevens ook voor toezicht en dienstverlening.

Wij gebruiken gegevens voor het heffen en innen van Rijksbelastingen, premieheffing volksverzekeringen en andere belastingen die moeten worden betaald. Voorbeelden van Rijksbelastingen zijn loon- en inkomstenbelasting, motorrijtuigenbelasting, erf- en schenkbelasting, overdrachtsbelasting, omzetbelasting, belastingen bij invoer van goederen, accijnzen. Dit doen we op basis van de Algemene wet inzake rijksbelastingen, de Invorderingswet en de verschillende belastingwetten.

De Belastingdienst gebruikt gegevens ook voor uitkeren van toeslagen. Het gaat om gegevens voor het berekenen van uw toeslagen en voor het uitbetalen daarvan. En als dat nodig is om teveel betaalde toeslagen van u terug te vragen. Het gaat om huurtoeslag, zorgtoeslag, kinderopvangtoeslag en kindgebonden budget. Dit doen we op basis van de Algemene wet inkomensafhankelijke regelingen en de verschillende toeslagenwetten.

De Belastingdienst neemt geen geautomatiseerde besluiten op basis van profilering in de zin van de AVG. De Belastingdienst maakt wel gebruik van persoonlijke aspecten om dossiers te selecteren voor toezicht op de juistheid van een aangifte of van een toegekende

toeslag. Dossiers die op die manier zijn geselecteerd worden altijd door een mens beoordeeld en die persoon neemt ook het besluit."

Zo kunnen betrokkenen hier lezen dat zij op grond van de AVG bepaalde rechten hebben, en op welke wijze zij hiervan gebruik kunnen maken. Zij kunnen de directie Toeslagen vragen om:

- a. inzage in de hem betreffende persoonsgegevens en een toelichting daarop (artikel 15 AVG)
- b. rectificatie van de hem/haar betreffende onjuiste persoonsgegevens (artikel 16 AVG);
en
- c. onder voorwaarden verwijdering van gegevens (artikel 17 AVG).

Betrokkenen kunnen overigens ook hun gegevens inzien via Mijn toeslagen. Elke wijziging die wordt opgevoerd voor de toekenning van de toeslag is hier zichtbaar, en ook staan hier alle gegevens waarop de toeslag is gebaseerd. Verzoeken van betrokkenen op grond van de AVG komen centraal binnen bij B/CAP, waarbij generieke inzageverzoeken centraal worden afgehandeld met een algemene brief. Specifieke inzageverzoeken en verwijderings- en correctieverzoeken worden doorgezet naar de directie Toeslagen. De reactie hierop is een voor bezwaar vatbaar besluit (artikel 34 Uitvoeringswet AVG). Het besluit wordt met ondersteuning van team Klacht genomen door (onder)gemandateerde medewerkers van team Vaktechniek, waarbij ook wordt beoordeeld of er beperkingen gelden op grond van artikel 23 van de AVG.

Specifiek over het Risicoclassificatiemodel:

- Recht op inzage in de verwerkingen: Dit is beperkt vanwege het feit dat als we het model prijsgeven is het niet meer mogelijk om effectief toezicht uit te voeren. Echter zouden betrokkenen informatie over de verwerking zonder alle details kunnen krijgen. Het inzagerecht kan in uitzonderingsgevallen geweigerd worden; bijvoorbeeld als er toezichtsbelangen spelen. (Zie Risico's en Maatregelen)
- Recht op informatie: de betrokkenen worden indirect én beperkt over het gebruik van het RCM geïnformeerd via de privacyverklaring die op de website van de belastingdienst staat. (Zie Risico's en Maatregelen)

Tekst:

De Belastingdienst neemt geen geautomatiseerde besluiten op basis van profilering in de zin van de AVG. De Belastingdienst maakt wel gebruik van persoonlijke aspecten om dossiers te selecteren voor toezicht op de juistheid van een aangifte of van een toegekende toeslag. Dossiers die op die manier zijn geselecteerd worden altijd door een mens beoordeeld en die persoon neemt ook het besluit.

De beperking van Informatie geldt op grond van art. 23 van de AVG en art. 41 van de uitvoeringswet AVG:

De verstrekende partij hoeft de betrokkene niet te informeren als:

- De betrokkene al op de hoogte is van de informatie die anders verstrekt wordt (art. 13 lid 4 AVG en art. 14 lid 5, aanhef en onder a, AVG);
- Het voldoen aan de informatieplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt overigens alleen als de gegevens niet bij de betrokkene zelf zijn verkregen);
- Zich een situatie voordoet waarbij het niet informeren van de betrokkene noodzakelijk en evenredig is voor bijvoorbeeld:
 - de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (art. 23 AVG jo. art. 41 lid 1, aanhef en onder d, UAVG);
 - een taak op het gebied van toezicht (art. 23 AVG jo. art. 41 lid 1 aanhef en onder h, UAVG), of
- Bezwaar maken tegen een besluit: Aanvragers kunnen bezwaar maken tegen het resultaat van de behandeling van hun aanvraag.
Het transparantieprincipe hoeft niet zo uitgelegd te worden dat iedere betrokkene specifiek over de registratie van een risicosignaal geïnformeerd wordt (art. 67 AWR regelt geheimhouding). Dit wordt echter anders zodra er nadelige gevolgen voor de betrokkene kunnen optreden of zijn opgetreden. Betrokkenen kunnen over de informatie beschikken waarop deze beslissingen zijn genomen, zodat hij daartegen bezwaar kan maken.
- Recht op beperking of beëindiging van de verwerking en recht op persoonsgegevens te verwijderen ('recht op vergetelheid'):
De inperking van deze twee rechten ontstaat als gevolg van de toelagaaanvraag. Zodra er een toelag is toegekend kan de toelagaaanvrager niet meer verzoeken om beperking of eindiging van de verwerking. Dit ligt aan het feit dat directie Toeslagen tot vijf jaar na afgifte definitieve beschikking een herziening mag afgeven op basis van nieuwe feiten. Daarnaast is het ook voor de toelagaaanvrager mogelijk om nog binnen vijf jaar na afgifte van een definitieve beschikking een verzoek om herziening aan te vragen. Ook het beperken van het recht op vergetelheid hangt hier mee samen.
- Recht om aan uitsluitend geautomatiseerde besluitvorming te worden onderworpen:
Het verwerken van persoonsgegevens in het risicoclassificatiemodel kwalificeert als profilering in de zin van artikel 4, aanhef en onder 4, van de AVG. Aanvragen die het risicoclassificatiemodel selecteert worden handmatig beoordeeld door een medewerker van Toeslagen. Er is door deze menselijke tussenkomst geen sprake van geautomatiseerde besluitvorming als bedoeld in artikel 22 van de AVG.

C. Beschrijving en beoordeling risico's voor de betrokkenen

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

16. Risico's



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

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

[Klik hier om infotekst te verbergen](#)

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- waar de gegevensverwerking kan leiden tot:
 - discriminatie, stigmatisering en uitsluiting;
 - (blootstelling aan) identiteitsdiefstal of -fraude;

- financiële verliezen;
 - reputatie- of anderszins relationele schade;
 - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
 - ongeoorloofde ongedaanmaking van pseudonimisering;
 - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.

Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij

sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.

Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

Nr.	Risico	Oorsprong	Kans ⁵⁴ (1-5)	Impact ⁵⁵ (1-5)
1.	Het risico kan ontstaan dat het resultaat onnauwkeurig en/of discriminerend is en dat het model niet meer representatief is.	Regressiemodellen moeten vaak getraind worden met actuele trainingcases, maar dit gebeurt niet altijd.	3	4 – Externe impact Proces: A, B Als het model de verkeerde indicatoren gebruikt dan bestaat de kans dat er burgers een onterecht hoge score van het model krijgen, wat een vertraging van het ontvangen van toeslag kan betekenen. Het heeft invloed op de toekenning van de betrokkene. Als er al een toekenning is en de burger stuurt een wijziging in dan wordt de wijziging niet verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd.
2.	Het risico kan ontstaan dat gegevens onrechtmatig worden gebruikt en dat er onnodig gegevens worden verzameld (gebrek aan dataminimalisatie).	Verwerking van gegevens die niet nodig zijn voor het model en waar geen doelbinding bestaat.	3	4 – Externe impact Proces: A, B Als er data onrechtmatig wordt gebruikt en dit is er de oorzaak van dat het een hogere score oplevert, dan zal de aanvraag naar Behandeling gaan, wat een vertraging van het ontvangen van toeslag kan betekenen. Het heeft invloed op de toekenning van de betrokkene. Als er al een toekenning is en de burger stuurt een wijziging in dan wordt de wijziging niet verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd.

⁵⁴ Kans op een schaal van 1 tot 5, waarbij 1 een lage kans is en 5 een hoge kans.

⁵⁵ Impact op een schaal van 1 tot 5, waarbij 1 een lage impact is en 5 een hoge impact.

3.	Het risico kan ontstaan dat de geselecteerde posten niet onrechtmatig zijn en dat de burger gestigmatiseerd wordt, en/of dat het langer duurt voordat de toekenning definitief beschikt wordt.	Posten met hoge risico score worden aan team Toezicht gestuurd voor behandeling.	2	4 – Externe impact Proces: A, B, C Het heeft invloed op de toekenning van de betrokkene. Als er al een toekenning is en de burger stuurt een wijziging in dan wordt de wijziging niet verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd.
4.	In relatie tot de posten die niet onrechtmatig verklaart en dan gaan binnen het VT/DT proces in: Op basis van het feit dat er een massale gegevensverwerking plaatsvindt en er geen mens aan te pas komt bij besluitvorming (geautomatiseerde besluitvorming) bestaat het risico dat er fouten worden gemaakt o.b.v. verkeerde of verouderde gegevens.	EDPB criterium: Geautomatiseerde besluitvorming AVG artikel 35	2	4 – Externe impact Proces: A, B, C Dit kan resulteren in de volgende privacyrisico's: - Betrokkenen kunnen een beschikking ontvangen met teveel of te weinig toeslag waardoor de betrokkenen moet terugbetalen
5.	Het risico kan ontstaan dat de verdeling in het model niet evenredig is (selectiebias).	Wij onderzoeken alleen de hoge scores en er is geen toezichtproces dat ook andere kenmerken onderzoekt. Er is momenteel geen capaciteit om valse negatieven te controleren.	3	3 – Externe impact Proces: A, B Impact is middelmatig. Bij het ontvangen van de definitieve toekenning kunnen burgers zien of ze te veel of te weinig voorschot hebben gekregen, of precies het juiste bedrag. Valse positieven zouden invloed op de toekenning van de betrokkene kunnen hebben. Als er al een toekenning is en de burger stuurt een wijziging dan wordt de wijziging niet direct verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd. Valse negatieven zouden een lage impact voor de burger kunnen hebben, tenzij het betrekking heeft op een aanvraag die gewijzigd zou moeten worden om terugvorderingen te voorkomen.

6.	Het risico kan ontstaan op het niet naleven van het transparantiebeginsel van de AVG.	De informatie in de privacyverklaring is beperkt	3	3 – Externe impact Proces: A, B, C De burgers zouden geen duidelijke informatie over de verwerking krijgen.
7.	Het risico kan ontstaan dat medewerkers in het kader van logging en monitoring gecontroleerd worden	Medewerkers worden gemonitord	3	3 – Interne impact Proces: A, B, C Mogelijke inbreuk op de privacy van medewerkers.
8.	Het risico kan ontstaan dat het resultaat niet aan de eisen van de opdracht voldoet.	De opdracht is niet altijd duidelijk door o.a. het gebrek aan specifieke doelstellingen	1	4 – Externe impact Proces: A, B Als het model de verkeerde indicatoren gebruikt dan bestaat de kans dat de verkeerde burgers een onterecht hoge score van het model krijgen, wat een vertraging van het ontvangen van toeslag kan betekenen. Het heeft invloed op de toekenning van de betrokkene. Als er al een toekenning is en de burger stuurt een wijziging in dan wordt de wijziging niet verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd.
9.	Het risico kan ontstaan dat de gegevens die verwerkt worden in het model niet altijd correct zijn.	Gegevens worden uit verschillende bronnen verzameld. Het is mogelijk dat de gegevens niet correct of geüpdatet vanuit de oorspronkelijke bron zijn ontvangen.	1	4 – Externe impact Proces: A, B De burgers zouden een onterecht hoge score kunnen krijgen wat een vertraging van het ontvangen van toeslag kan betekenen. Het heeft invloed op de toekenning van de betrokkene. Als er al een toekenning is en de burger stuurt een wijziging in dan wordt de wijziging niet verwerkt en is deze ook niet zichtbaar voor de burger. Pas na handmatige controle en goedkeuring door een medewerker wordt de wijziging doorgevoerd.
10.	Het risico kan ontstaan dat de output van het model niet meer uitlegbaar is, wat een probleem zal vormen op het moment dat een burger zijn recht op inzage wil uitoefenen.	De logica van het model kan complex zijn. De risicoscore per indicator is niet altijd uitlegbaar.	2	3 Externe impact Proces: A, B, C De burgers zouden geen duidelijke informatie over de verwerking krijgen en het zou

				kunnen dat ze niet begrijpen waarom hun aanvraag als hoog risico is geselecteerd.
11.	Het risico kan ontstaan dat er per ongeluk gegevens naar een verkeerd e-mailadres verstuurd worden. Het gaat met name over een intern datalek binnen directie Toeslagen.	Gegevens worden vaak per e-mail verstuurd. Op dit moment kan DAT niet extern mailen, maar andere afdelingen wel.	2	3 – Interne impact Proces: A, B, C Als de gegevens lekken en/of worden misbruikt dan zou dat impact op de reputatie van de burger kunnen hebben. De impact is middelmatig omdat de output bestanden bevatten alleen BSN nummers en geen andere persoonsgegevens.
12.	Het risico kan ontstaan op een inbreuk op het beginsel van opslagbeperking.	Gegevens worden te lang bewaard en er is geen vernietigingsproces voor de Q-schijf en SAS.	3	2 – Interne impact Proces: A, B, C Impact is laag voor de burger omdat de gegevens intern blijven.
13.	Het risico kan ontstaan dat medewerkers toegang hebben tot informatie die zij niet (meer) nodig hebben om hun werk te kunnen doen.	Autorisatiebeleid kan strenger zijn voor bepaalde producten binnen SAS en de Q-schijf.	2	2 – Interne impact Proces: A, B De informatie blijft intern dus de impact voor de betrokkene is zeer laag.

D. Beschrijving voorgenomen maatregelen

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

17. Maatregelen



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

De informatiebeveiliging en de adequaatheid van de maatregelen zullen door de CISO worden beoordeeld.

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

- a. pseudonimiseren en versleutelen van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;

- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

- a. controle op de toegang tot de apparatuur;
- b. controle op de gegevensdragers;
- c. opslagcontrole;
- d. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelmogelijkheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Risico nr.	Maatregelen	Restrisico	Restrisico geaccepteerd
1	- Het model regelmatig trainen en testen: één keer voor dat het model gaat draaien en daarna iedere 2 maanden Werk: +- 200 uur/jaar (DAT en HHR) - Oude trainingcases verwijderen. Statistisch checken of er verschillen zijn. In dat geval dmv steekproeven de nauwkeurigheid van het model meten Werk: +- 8 uur (DAT) en 50 uur HH1 en Productieregie. Planning: Q2 2021	Capaciteit is niet altijd beschikbaar. Oplossing: minimaal 20% capaciteit posten nodig voor aselecte. Een team zou voor een keer per maand beschikbaar moeten komen.	☒
2	Gegevens periodiek reviewen en toetsen op dataminimalisatie en grondslag. Check op aanwezigheid van proxies. Waar nodig gegevens niet meer als bron gebruiken en het model hertrainen. Een audit proces vastleggen en goed documenteren. Werk: +-100 uur (DAT), +-50 uur (HHR) Planning: Q2 2021	Het model kan minder voorspellend worden. Actie: behandelen/wachten/trainen	☒
3	Met de Implementatie van de rest van de maatregelen zal dit risico verminderd worden.	Er zal altijd een risico bestaan dat een klein percentage posten valse positieven of valse negatieven zijn. Door middel van techniek kunnen wij het risico altijd verminderen maar niet helemaal mitigeren.	☒
4	Burgers worden geïnformeerd in de privacy statement over de geautomatiseerde besluitvorming. Daarnaast zijn de volgende waarborgen ingeregeld: periodiek reken- en bedrijfsregels testen, qa/qc inrichten (rechtmatigheid toetsen zowel intern - Team rechtmatigheidstoetsen als door de ADR), auditen van uitkomsten door de ADR, openstaan voor vragen van betrokkenen,	Restrisico is minimaal. Burgers lezen niet wat er in het privacy statement is opgenomen. Een mogelijke restmaatregel is om dit prominenter "aan te	☒

	menselijke tussenkomst organiseren d.m.v. vraag, bezwaar en inzage.	bieden" aan te burger bij het invullen van gegevens en/of het in laagdrempelig begrijpelijk Nederlands te vermelden.	
5	- Steekproeven gebruiken voor het trainen van het model en gestratificeerde aselechte steekproef uitvoeren voor het vinden van nieuwe cases. Ook naar de lagere scores kijken om evenredigheid te garanderen. Op deze manier worden ook mogelijke valse negatieven gecontroleerd. - Iedere 6 maanden overwegen of de aselechte nodig is als er veranderingen ontstaan in het patroon. - Meer capaciteit inzetten voor het checken van de 20% groene posten, Hiermee wordt het model niet alleen getoetst op onderscheidend vermogen, maar ook getraind op rechtmatige cases. Werk: binnen de uren ingeschat voor risico 1.		n.v.t
6	Vanuit directie Toeslagen wordt het initiatief opgepakt om samen met IV&D te bekijken in welke mate het privacy statement van de Belastingdienst, zoals gepubliceerd op belastingdienst.nl, moet worden aangepast. Indien een aanpassing noodzakelijk blijkt wordt een tekstvoorstel met verzoek tot aanpassing ingediend. Daarnaast komt een addendum voor Toeslagen op de privacyverklaring van de directie Toeslagen. Risico eigenaar: Toeslagen. Planning: Q2 2021		n.v.t
7	Er is instemming met OR geweest op grond van art. 27, lid 1, onder k en l, Wet op de ondernemingsraden (Wor). (zie bijlage)		n.v.t
8	Steekproef uitvoeren. Deze is onderdeel van de maatregelen uit risico 1. Uit de steekproef moet naar voren komen wat de doelstellingen zijn.		n.v.t
9	Er zijn afspraken met de leveranciers van de gegevens mbt de actualiteit van de gegevens. Toch is er altijd een risico dat de gegevens die niet uit de BRP (basis registratie) komen niet correct of geüpdatet vanuit de oorspronkelijke bron zijn ontvangen. Dit risico is heel laag en het wordt geaccepteerd.		n.v.t.

10	DAT heeft een Privacy by Design training gekregen (en er volgen nog een paar sessies) waar analisten leren om dit risico te identificeren en te behandelen. Daarnaast is DAT bezig om interne processen en checklijsten te creëren om o.a. dit soort risico's te voorkomen.		n.v.t
11	De nieuwe werkwijze van Analytics United zal dit risico mitigeren. Naar verwachting wordt het in Q2 2021 geïmplementeerd (zie bijlage met nieuw proces)	Het risico blijft ontstaan tot de maatregel geïmplementeerd wordt.	☒
12	- Het implementeren van een proces om de gegevens te vernietigen gebaseerd op de Selectielijst. Hiervoor loopt het project informatie huishouding (voor e-mail en Q-schijf). - Maatregelen implementeren voor het vernietigen van gegevens in SAS: Werk: +- 24 uur (DAT). Sessies inplannen om te overleggen, maatregelen vastleggen, met afstemmen en acties ondernemen. Planning: Q2 2021		n.v.t
13	Een duidelijk en strenger autorisatiebeleid voor het RCM team implementeren. Audit-trail is al geïmplementeerd voor SAS. Risico eigenaar: DAT Deadline: het wordt geïmplementeerd vóór de volgende run.		n.v.t

Aanvaardbaarheidscriteria bij de acceptatie van restrisico's:

Een restrisico is acceptabel in geval van:

- laag risico;
- tijdelijkheid van het risico afhankelijk van het risico en de te nemen maatregelen;
- onduidelijkheid over interpretatie van de norm die grotendeels bepalend is voor het risico, terwijl de gekozen interpretatie door bijvoorbeeld een gezaghebbende uitspraak of advies als verantwoord is te beschouwen;

Een restrisico is niet acceptabel in geval van:

- hoog risico;
- overtreding van de wetgeving.

Is een voorafgaande raadpleging door de Autoriteit persoonsgegevens nodig?

Momenteel is raadpleging door de AP niet nodig. Als na de implementatie van de maatregelen mogelijke nieuwe risico's en restrisico's in kaart zijn gebracht, zal dit besluit opnieuw bekeken worden.

Bijlage 1:

Bronnen gebruikt in het risicoclassificatiemodel:

Bronnen	Omschrijving	Oorspronkelijke bron	Ontvangsmethode	Opslag
6PP	Tabel met alle geldige postcodes in Nederland, inclusief lengte- en breedtegraad	d-centralize.nl	Csv-bestand gedownload	Q-schijf en SAS
BAG	Basisregistratie adressen en gebouwen	CIV	Csv-bestand per e-mail	Q-schijf en SAS, e-mail
Beschikkingen HT	Lijst met formele HT beschikkingen en de details hiervan	CIV	SAS-bestand	SAS
Beschikkingen KOT	Lijst met formele KOT beschikkingen en de details hiervan	CIV	SAS-bestand	SAS
Betrokkenen HT	Lijst met betrokken BSN's per formele HT beschikking	CIV	SAS-bestand	SAS
Bezwaren	Lijst met BSN's waarvoor recent door de directie Toeslagen een bezwaar is afgehandeld (stellaposten)	Stella team	xlsx-bestand per e-mail	Q-schijf, SAS, e-mail
BVR	Beheer van relaties: adressenbestand van de directie Toeslagen, mede gevoed door GBA en BRP, met persoonsdetails.	via het datafundament	SAS-bestand	SAS
COA	Centrale Ontvangers Administratie - BSN's met openstaande vorderingen bij de Belastingdienst	CAP (team Inning)	SAS-bestand via de Q-schijf	SAS, Q-schijf
Deeljaar beschikking HT	Details van HT beschikkingen per deel van het toeslagjaar.	CIV	SAS-bestand	SAS
Deeljaar beschikking KOT	Details van KOT beschikkingen per deel van het toeslagjaar.	CIV	SAS-bestand	SAS
Excepties	Lijst met BSNs die niet uitgesloten mogen worden.	HHR	xlsx-bestand per e-mail	Q-schijf,

			mail op de dag van de definitieve run	SAS, e-mail
Holland2stay	Lijst met aanvragen HT van buitenlandse studenten. Doel: horizontaal toezicht (BSN's op de lijst worden niet gecontroleerd omdat de verhuurder heeft dat al gedaan).	Woningbouwvereniging Holland2Stay	xlsx-bestand per e-mail een dag voor de definitieve run	Q-schijf, SAS, e-mail
Hot Hor	Lijst van BSN's waarvoor in TVS een actuele conceptbeschikking met een hoog bedrag (dus een hoog risico) klaarstaat en waarvoor nog geen handmatige controle is toegepast.	KPT_Werkopdracht view uit het datafundament	SAS-bestand	SAS
IGS	Lijst van BSN's die de IGS (ingebrekestelling) status hebben.	KPT_Werkopdracht view uit het datafundament	SAS-bestand	SAS
KOT conceptbeschikkingen	Lijst met formele KOT conceptbeschikkingen en de details hiervan	CIV	SAS-bestand	SAS
LRK	Register van Kinderopvang instellingen	DUO via CAP	Txt-bestand op de Q-schijf	Q-schijf en SAS
Meldingen FRS	Verzameling van door TVS gegenereerde meldingen.	CIV	SAS-bestand	SAS
Onbekende aanvragers (nieuwe aanvragers)	Lijst van BSN's die minder dan 1 jaar oud zijn, waarvoor nog nooit een formele beschikking met een bedrag > 0 is uitgereikt en waarvoor nu een conceptbeschikking met bedrag > 0 klaarstaat. De brondata wordt gebruikt in het halfproduct 'Uitsluitlijst onbekende aanvragers Zorg'.	CIV	SAS-bestand	SAS
Ouder_Kind	Matrix met relaties tussen BSN's van ouders en BSN's van hun kinderen	CIV	SAS-bestand	SAS
Uitgesloten adressen	Lijst van fysieke adressen waarvoor geen recht op huurtoeslag mogelijk is.	Toeslagen verhuurder administratie_Po stbus	xlsx-bestand per e-mail	Q-schijf, SAS, e-mail
Uitsluitlijst	Actuele lijst van BSN's waarvoor toeslagrecht over een bepaalde periode is geblokkeerd.	CIV	SAS-bestand	SAS
Uitval	Lijst van in TVS ontbrekende informatie op een of meerdere toeslagaanvragen per BSN	TQL (TVS)	Txt-bestand op SAS Grid	SAS
VHA	Verhuurders Administratie - door directie Toeslagen opgestelde lijst van huurbedragen per fysiek adres volgens verhuurders.	CIV	SAS-bestand	SAS
VIP	Lijst van binnen de directie Toeslagen beschermde BSN's die niet voor elke behandelaar inzichtelijk zijn. De brondata wordt gebruikt in halfproducten HT_Model en KOT_Model.	CIV	SAS-bestand	SAS
Vluchtelingenwerk	Lijst met huurtoeslagaanvragen voor vluchtelingen, aangevraagd door de organisaties Vluchtelingenwerk en COA ⁵⁶ (Centraal Orgaan opvang Asielzoekers). Doel: horizontaal toezicht (BSN's op de lijst worden niet gecontroleerd omdat de COA heeft dat al gedaan).	CIV	SAS-bestand	SAS
Wanbetalers	Lijst met BSN's waarvan vanuit CVZ bekend is dat geen zorgpremie wordt afgedragen.	CIV	SAS-bestand	SAS
WOZ	Lijst van actuele onroerend goed bezittingen per	CIV	SAS-bestand	SAS

⁵⁶ Convenant: https://download.belastingdienst.nl/toeslagen/docs/conv_toeslagen_coa_tg10001z1ed.pdf

	BSN			
--	-----	--	--	--

Bijlage 2:

Halfproducten gebruikt in het risicoclassificatiemodel:

Halfproducten	Omschrijving
6PP	Tabel met alle geldige postcodes in Nederland, inclusief lengte- en breedtegraad
BAG	Basisregistratie adressen en gebouwen
Bezwaren	Lijst met BSN's waarvoor recent door de directie Toeslagen een bezwaar is afgehandeld.
BVR	Beheer van relaties: adressenbestand van de directie Toeslagen, mede gevoed door GBA, met persoonsdetails.
COA	Tabel met BSN's die een openstaande vorderingen hebben bij de directie Toeslagen.
DTM_HT	In deze flow worden de beschikkingen plat geslagen tot een tabel op deeljaar niveau. Hieraan worden de conceptbeschikkingen toegevoegd, en vervolgens gekoppeld aan de (inkomens) van betrokkenen.
DTM_KOT	In deze flow worden de beschikkingen plat geslagen tot een tabel op deeljaar niveau. Hieraan worden de conceptbeschikkingen toegevoegd, en vervolgens gekoppeld aan een aantal halfproducten.
Holland2stay	Lijst met aanvragen HT van buitenlandse studenten.
Hot Hor	Lijst van BSN's waarvoor in TVS een actuele conceptbeschikking met een hoog bedrag staat.
IGS	Selectie gemaakt op de werkitens mbt een ingebrekestelling en met status niet completed.
LRK	Tabel met kinderopvangstelling en een aantal details daarvan volgens het landelijk register.
Melding8	Tabel met 'meldingen 8' (nieuwe toeslagaanvraag) uit TVS per BSN.
MeldingFRS	Tabel met aantal opgegeven verhuizingen (melding 6), aantal veranderde betaalwijzen per jaar (melding 15), aantal wijzigingen in aantal uren opvang per jaar (melding 18), aantal wijzigingen in de huurprijs (melding 19) per BSN.
Ouder_Kind	Tabel met BSN's van de ouder(s) per kind.
Uitgesloten adres	Tabel met adressen waarvoor geen toeslagrecht bestaat.
Uitsluiten_onbekende_aanvragers_zorg	Lijst van BSNs met afgewezen aanvragen zorgtoeslag in de afgelopen jaren (geen recht vanwege buitenlands adres). Dit halfproduct wordt niet in het RCM gebruikt maar in het project Zorgverzekerd.
Uitsluitlijst	Tabel met BSN's die op een gegeven moment in de tijd uitgesloten worden van beschikkingen voor een bepaalde toeslageregeling.
Uitval	Lijst van in TVS ontbrekende informatie op een of meerdere toeslagaanvragen per BSN
VHA	Verhuurders Administratie - door directie Toeslagen opgestelde lijst van huurbedragen per fysiek adres volgens verhuurders.
Vluchtelingenwerk	Lijst met aanvragen HT door vluchtelingen
WOZ	Lijst van actuele onroerend goed bezittingen per BSN

Bijlage 3:**Indicatoren HT:**

Label	Omschrijving	Bron
KALE_HUUR	Huurprijs exclusief de servicekosten	DTM_HT
aantal_htuitval53	Is er opgegeven of er een medebewoner is?	SAS
av_aant_vorderingen	Heeft de directie Toeslagen een vordering op deze persoon?	SAS
av_adr_aant_inschrijvingen	Hebben we het aantal ingeschrevenen kunnen bepalen?	SAS
av_groei_inkomen	Hebben we de groei van het inkomen kunnen vaststellen?	SAS
draagkracht_ht	Hebben we de draagkracht vast kunnen stellen?	SAS
opg_totale_huur	Is de totale huur bekend?	SAS
oppervlakte_per_persoon	Oppervlakte per persoon	HT_MODEL
oppervlakteprijs	Huurprijs per vierkante meter	HT_MODEL
perc_huur_draagkracht	Ratio huurprijs tov draagkracht	HT_MODEL
perc_huur_VHA_huur	Verschil huurprijs opgeven VHA en verhuurder	HT_MODEL
perc_huurprijs_huurprijs_omg	Huurprijs t.o.v. huurprijs in omgeving	HT_MODEL
perc_huur_tov_huurgrens	Huurprijs t.o.v. huurgrens	HT_MODEL
TERUGWERKENDE_KRACHT	Mate van terugwerkende kracht (obv melding 8) aangevraagd door (niet namens) burger zelf.	Melding8

Indicatoren HT die niet meer worden gebruikt: de volgende indicatoren zijn op reject gezet in het model, echter worden de brongegevens verwerkt in de data preparatie. Die zal in Q2 2021 structureel uit het model verwijderd worden. (zie Risico 2 in hoofdstuk 16 "Risico's" en 17 "Maatregelen")

Label	Omschrijving	Bron
av_adr_aant_kinderen	Aantal ingeschreven kinderen op adres - volgens GBA	BVR
av_adr_aant_volwassenen	Aantal ingeschreven volwassenen op adres - volgens GBA	BVR
av_elgenaar_pand	Of de aanvrager/toeslagpartner van een toeslag ook elgenaar is van dat pand	HT_MODEL
Huur_deelbaar_door_10	Huurprijs deelbaar door 10?	DTM_HT
Huur_deelbaar_door_50	Huurprijs deelbaar door 50?	DTM_HT
aant_wijz_huurprijs_burger	Indicatie of het bekend is hoe vaak de burger zijn huurprijs aangepast heeft	SAS
aantal_betrokkenen	Indicatie of het aantal betrokkenen is opgegeven	SAS
aantal_htuitval	Is er sprake van een onvolledig ingevulde aanvraag?	SAS
av_aant_verhuiz_opgegeven	Hoeveel verhuizingen zijn er door de burger opgegeven?	SAS
av_aant_verhuizingen_gba	Hoe veel verhuizingen zijn er volgens het GBA bij deze aanvrager?	SAS
av_inkomen_ht	Hebben we het inkomen kunnen vaststellen?	SAS
av_leeftijd_bsn	Hebben we de leeftijd van de aanvragers BSN kunnen vaststellen?	SAS
av_nationaliteit*	Hebben we de nationaliteit van de aanvrager kunnen vaststellen? Nederlandschap ja/nee (waarden 0 en 1). * Deze gegevens zullen in Q2 2021 worden verwijderd.	SAS
av_woont_in_nl	Hebben we vast kunnen stellen of de aanvrager in Nederland woont?	SAS
av_openstaande_vorderingen	Hebben we openstaande vorderingen gevonden?	SAS
av_status_vorderingen	Hebben we de status van vorderingen kunnen vaststellen?	SAS
overleden	Is persoon overleden?	HT_MODEL
perc_oppervlakteprijs_omg	Oppervlakteprijs t.o.v. oppervlakteprijs in de omgeving	HT_MODEL
totale_service_kosten	Hoe hoog zijn de totale service-kosten?	DTM_HT
wanbetalen_zorg	Indicatie of bij CVZ bekend is dat geen zorgpremie wordt afgedragen voor	HT_MODEL

	betreffende BSN. * Deze gegevens zullen in Q2 2021 worden verwijderd.	
--	---	--

Bijlage 4:**Indicatoren KOT:**

Label	Omschrijving	Bron
aant_kinderen_in_opvang	Aantal kinderen waarvoor KOT is aangevraagd per BSN van de ouder.	DTM_KOT
afst_adr_opvang	Afstand in kilometers tussen huisadres aanvrager en adres van de kinderopvang volgens LRK.	DTM_KOT, LRK
av_aant_verhuizingen_gba	Aantal verhuizingen volgens de BVR.	BVR
av_aant_vorderingen	Aantal vorderingen per BSN.	COA
av_adr_aant_kinderen	Aantal Ingeschreven kinderen per adres volgens de BVR.	BVR
av_adr_aant_volwassenen	Aantal ingeschreven volwassenen per adres volgens de BVR.	BVR
av_groei_inkomen	Groei van het jaarinkomen (inkomen TVS tov inkomen BVR). Dit ligt tussen -5 en 5.	KOT_Model.Merge_BSN, DTM_KOT, BVR
av_leeftijd_bsn	Leeftijd BSN (tov) gewenste ingangdatum (uit aanvraag). Om te bepalen hoe lang iemand al in Nederland is. Het zal in Q2 2021 structureel uit het model verwijderd worden. (zie Risico 2 in hoofdstuk 16 "Risico's" en 17 "Maatregelen")	DTM_KOT, BVR
av_missend_voorgaande_ink	Indicatie of inkomen missend is in BVR.	KOT_Model.Merge_BSN, BVR
av_nul_inkomen_opgegeven	Indicatie of opgegeven inkomen in TVS nul is.	KOT_Model.Merge_BSN, DTM_KOT
av_openstaande_vorderingen	Bedrag aan openstaande vorderingen per BSN.	COA
av_recht_op_kgb	Indicatie of aanvrager of partner recht heeft op KGB voor alle kinderen volgens informatie van SVB.	DTM_KOT
av_status_vorderingen	Status van de openstaande vordering(en) volgens COA.	DTM_KOT
draagkracht_KOT	Draagkracht van het huishouden volgens TVS waartoe BSN volgens TVS behoort.	DTM_KOT
Eigen_bijdrage_per_maand	Verschil tussen aangevraagde uren aangevraagd tarief - de toegewezen toeslag.	DTM_KOT
leeft_oudste_kind	Leeftijd van het oudste kind waarvoor KOT wordt aangevraagd volgens BVR.	DTM_KOT
Leeftijd_bij_geboorte	Leeftijd van de aanvrager volgens de BVR op het moment van de toeslagaanvraag.	DTM_KOT
Max_uren	Aantal uur dat de aanvrager (minst werkende partner) zou moeten werken per maand om aantal aangevraagde uren kinderopvang te rechtvaardigen	KOT_Model.Merge_BSN
ouder_kind_rel_mist	Indicatie of volgens BVR geen sprake is van ouder-kind relatie tussen aanvrager of partner van de aanvrager en het kind waarvoor KOT wordt aangevraagd.	DTM_KOT
perc_inkomen_eigen_bijdrage	Percentage van het door de aangever opgegeven inkomen volgens zelf uitgegeven wordt aan opvang	DTM_KOT
terugwerkende_kracht	Aantal dagen tussen datum waarop toeslag is aangevraagd en de ingangsdatum van het tijdvak waarop de aanvraag betrekking heeft.	
uitval_kot	Aantal uitvalmeldingen in TVS voor de actuele toeslagaanvraag KOT.	KOT_Model.Merge_BSN
heeftpartner	Geeft aan of de aanvrager een partner heeft of niet.	CONCEPTBESCHIKKINGEN_KOT

Indicatoren KOT die niet meer worden gebruikt: de volgende indicatoren zijn op reject gezet in het model, echter worden de brongegevens verwerkt in de data preparatie. Die zal in Q2 2021 structureel uit het model verwijderd worden. (zie Risico 2 in hoofdstuk 16 "Risico's" en 17 "Maatregelen")

Label	Omschrijving	Bron
aantal_deel jaren	Aantal delen waaruit het toeslagjaar voor de betreffende BSN bestaat.	DTM_KOT
av_07_01_adr_niet_gelijk	Indicatie of '07 adres' (directie Toeslagen) niet gelijk is aan '01 adres' (BVR): bij 1 zijn adressen niet gelijk, anders 0.	BVR
av_aant_verhuiz_opgegeven	Aantal verhuizingen opgegeven in TVS.	MeldingFRS
av_adr_aant_inschrijvingen	Aantal inschrijvingen per adres volgens de BVR.	BVR
av_adr_gelijk_aan_ov_adr	Indicatie of adres van opvanglocatie gelijk is aan adres	DTM_KOT, LRK
av_ht_uitgesloten_adres	Adres uitgesloten voor HT volgens halfproduct Uitgesloten adres.	Uitgesloten adres
av_leeftijd	Leeftijd van de aanvrager volgens BVR	BVR
av_nationaliteit	Nationaliteit cluster van de aanvrager (1 = Nederlander, 0 = niet Nederlander) volgens de BVR. * Deze gegevens zullen in Q2 2021 worden verwijderd.	KOT_Model.Merge_BSN, BVR
av_verschil_verhuizingen	Verschil tussen aantal in TVS opgegeven verhuizingen en aantal verhuizingen volgens de BVR.	KOT_Model.Merge_BSN, MeldingFRS, BVR
av_woont_niet_in_nlbedu	Indicatie of aanvrager in Nederland, België of Duitsland woont.	KOT_Model.Merge_BSN, BVR
ind_bso_go	Indicatie of toeslagaanvraag betrekking heeft op buitenschoolse opvang door een gastouder	DTM_KOT
ind_bso_kc	Indicatie of toeslagaanvraag betrekking heeft op buitenschoolse opvang door een kindercentrum	DTM_KOT
ind_do_go	Indicatie of toeslagaanvraag betrekking heeft op dagopvang door een gastouder	DTM_KOT
ind_do_kc	Indicatie of toeslagaanvraag betrekking heeft op dagopvang door een kindercentrum	DTM_KOT
kind_niet_in_NLBEDU	Indicatie of het kind waarvoor KOT wordt aangevraagd volgens de BVR woonachtig is in Nederland, België of Duitsland	DTM_KOT
kind_woont_bij_av	Indicatie of het kind waarvoor KOT wordt aangevraagd volgens de BVR woonachtig is bij de aanvrager	DTM_KOT
leeft_jongste_kind	Leeftijd van het jongste kind waarvoor KOT wordt aangevraagd volgens BVR.	DTM_KOT
leeftijd_BSN_kind	Tijd tussen het aanmaakmoment van de BSN van het kind waarvoor KOT wordt aangevraagd volgens de BVR en de ingangsdatum van de toeslagaanvraag.	DTM_KOT
leeftijd_ov_issues	Indicatie of de leeftijd van het kind volgens BVR waarvoor KOT is aangevraagd overeen komt met het type opvang (yes/no)	DTM_KOT
max_uren_bso	Aantal uur dat de aanvrager (minst werkende partner) zou moeten werken per maand om aantal aangevraagde uren kinderopvang te rechtvaardigen	DTM_KOT
max_uren_do	Het hoogste aantal uren dagopvang voor 1 kind in de toeslagaanvraag.	DTM_KOT
max_uurtarief_bso	Het hoogst opgegeven uurtarief voor buitenschoolse opvang in de toeslagaanvraag.	DTM_KOT
max_uurtarief_do	Het hoogst opgegeven uurtarief voor dagopvang in de toeslagaanvraag.	DTM_KOT

pa_dagtaaktype	Dagtaaktype van de toeslagpartner als bekend in TVS.	DTM_KOT
Te_Jong_Voor_BSO	Indicatie of kind waarvoor toeslag voor buitenschoolse opvang is aangevraagd te jong is voor recht op toeslag voor buitenschoolse opvang.	DTM_KOT
Te_Oud_Voor_BSO	Indicatie of kind waarvoor toeslag voor buitenschoolse opvang is aangevraagd te oud is voor recht op toeslag voor buitenschoolse opvang.	DTM_KOT
Te_Oud_Voor_DO	Indicatie of kind waarvoor toeslag voor dagopvang is aangevraagd te oud is voor recht op toeslag voor dagopvang.	DTM_KOT
wanbetalen_zorg	Indicatie of bij CVZ bekend is dat geen zorgpremie wordt afgedragen voor betreffende BSN. * Deze gegevens zullen in Q2 2021 worden verwijderd.	KOT_Model.Merge_BSN
zelfde_kind_do_en_bso	Indicatie of voor hetzelfde kind over hetzelfde tijdvak zowel toeslag dagopvang als voor kinderopvang aangevraagd wordt.	DTM_KOT
Heeftbijstand (Hoogte)	Geeft aan of de aanvrager bijstand heeft of niet. * Deze gegevens zullen in Q2 2021 worden verwijderd.	FLG

Bijlage 5:

Control Matrix gebruikt voor kwaliteitscontrole van het model.

Voorbeeld van een deel van de control matrix:

Subproces	Controle
Trainingscases CSV	CSV bestand met trainingscases is correct geupdated met meest recente trainingscases. Denk aan: is datum beoordeeld juist ingevuld?
Initialize	Bij toevoeging van een nieuwe maand is een nieuwe library aangemaakt in script A01.
Initialize	Het bestand met trainingscases wordt correct ingelezen (script A02).
Initialize	Bij toevoeging van een nieuwe maand is deze maand toegevoegd aan samenvoeging gescoorde cases in script A03.
Create testcases	Bij toevoeging van een nieuwe maand is een nieuwe process flow toegevoegd.
Create testcases	Bij toevoeging van (een) nieuwe indicator(en) zijn deze voor alle historische runs op correcte wijze toegevoegd.
Append	Bij toevoeging van een nieuwe maand is deze maand toegevoegd aan samenvoeging trainingscases in script Z01.
Append	Alle overbodige kolommen worden gedropt in script Z01.
Append	Uit de controle in script Z02 volgen geen missings op indicatoren die niet missing mogen zijn.
Miner - Data Partition	Alle aangeleverde trainingscases worden gebruikt voor het trainen of het valideren van het model. Vergelijk aantal records HT_training en KOT_training met aantal regels in Enterprise Miner.
Miner - Scorecard	De door het model geselecteerde indicatoren, hun groepering en de hieraan gekoppelde scorecard points zijn plausibel.
Miner - Scorecard	De samenstelling van het model vertoont geen onverklaarbare of implausibele verschillen met het model van de vorige run.
#	Proces
Controle	
Wle	
1.1.	Brondata
Het aanleverformat (bestandsvorm, scheidingsteken, tekst qualifiers) is conform de in documentatie gegeven specificaties.	
1.2.	Brondata
Alle benodigde kolommen zijn beschikbaar.	
1.3.	Brondata
Het regelaantal is conform verwachting en in lijn met eerdere dataleveringen.	
1.4.	Brondata
Aantal regels in bronbestand = aantal regels in SAS	
1.5.	Brondata
In SAS zijn dataformats (denk aan: veldlengte, decimalen, datumformat) goed geladen	
2.1.	Halfproduct
Brondata is ververs	
2.2.	Halfproduct
Er zijn na het draaien van het halfproduct geen errors/uninitialized/kritieke warnings in log.	
2.3.	Halfproduct
De output is conform verwachting: vereiste kolommen zijn beschikbaar en hebben plausibele waarden, regelaantal is conform verwachting.	
2.4.	Halfproduct
Geen missings op (numerieke) indicatoren die niet missing mogen zijn.	
2.5.	Halfproduct
Filter op 'datum einde' in halfproduct bewaren is correct gezet (in het algemeen: net voor vorige run van betreffende toeslagjaar).	
Algemeen	
3.1.	Productie
Voordat productierun wordt gestart zijn alle historische halfproducten verwijderd.	
3.2.	Productie
Voordat productierun wordt gestart zijn alle actuele halfproducten naar de laptop gekopieerd.	

Bijlage 6: OR Instemmingsverzoek monitoring DF&A (Zie bijgevoegd pdf bestand)

Bijlage 7: Analytics United proces

Procesbeschrijving

In dit onderdeel volgt een beschrijving van het proces vanaf een *aanvraag/opdracht* * van een klant tot de oplevering van een product binnen het virtuele team Analytics United.

Uitgangspunten

Op dit moment zijn er drie belangrijke uitgangspunten gedefinieerd, namelijk:

1. De processen, maatregelen en acties gevraagd door en voor het programma Analytics United zijn niet blokkerend voor de productie van de Toeslagen analytics teams en medewerkers (een tijdige uitlevering staat voorop).
2. **Alle** opdrachten/aanvragen* (hoe groot of klein ze zijn) worden naar de portfoliopostbus (Toeslagen AU Portfoliomanagement Postbus) gestuurd.
3. Voor alle producttypen (behalve datafundament) houd je als self-assessment een QC-vragenlijst bij tijdens ontwikkeling. Deze mail je naar Toeslagen AU Quality Control Postbus zodra je klaar bent met ontwikkelen en op het punt staat het eindresultaat uit te leveren.

*Onder aanvraag/opdracht verstaan we de ontwikkeling van een gegevensproduct, Eenmalige Analyse, Rapportage of Dashboard en signaalmodel of risicomodel. Hierbij worden gegevens verwerkt en als eindresultaat opgeleverd. Het beantwoorden van een vraag waarvoor geen nieuwe gegevens verwerkt of opgeleverd hoeven te worden, valt buiten beschouwing en hoeft niet te worden aangemeld. Werkzaamheden met betrekking tot de zogenaamde 'schermrobot' zijn hier ook van uitgesloten.

Processtappen

Stap 1

De opdrachtgever vult, eventueel in samenwerking met de analist, het intakeformulier in met een aanvraag voor het ontwikkelen van een nieuw product of wijziging op een bestaand product. De opdrachtgever is verantwoordelijk voor het correct invullen van het intakeformulier. Vervolgens moet dit volledig ingevulde intakeformulier naar de Toeslagen AU Portfoliomanagement Postbus gestuurd worden.

Het portfoliomanagement maakt een epic aan op het TSPM bord met de status 'Intake'.

Stap 2

Het intakeformulier omvat de intake, risicoclassificatie en privacy proces. De analist doorloopt het privacy proces (D-23). Als contact met een privacy coördinator nodig of gewenst is, kan er gebeld worden met IBP. De emailadressen zijn te vinden op de homepage.

De analist kan vervolgens direct met de aanvraag aan de slag. Houd hierbij rekening met de planning en prioriteit van opdrachten. Wanneer een analist begeleiding met het werken volgens standaarden en richtlijnen wil ontvangen, kan Quality Assurance (QA) begeleiding door de analist aangevraagd worden. Hiervoor geldt deze werkinstructie. Stuur de aanvraag naar de Toeslagen AU Quality Control Postbus.

Wanneer de analist de opdracht in behandeling neemt, zet hij of zij dit epic op het TSPM bord in fase 'Delivery'. De analist is gedurende de ontwikkeling van het product verantwoordelijk voor het aanpassen van de faseovergangen op het TSPM bord in Jira.

Stap 3

De analist houdt tijdens het ontwikkelen van het product het QC-formulier voor Toeslagen bij (behalve voor datafundamenten). De analist houdt zich aan de standaarden in dit formulier tijdens de ontwikkeling. Bijvoorbeeld het 4-ogen principe (T-48), veilig versturen (T-31) en het privacy proces (D-23).

De analist draagt er zorg voor dat alle relevante documentatie bij een opdracht op een veilige locatie wordt opgeslagen. Een overzicht van relevante documentatie staat in de onderstaande tabel. Het staat de analist vrij om te kiezen waar en met welke nummering of benaming de documentatie opgeslagen wordt, echter moet het bijbehorende TSPM of TSEX nummer altijd te achterhalen zijn, ten behoeve van QC.

Altijd vereist	Vereist indien van toepassing
Intakeformulier	Solution Design & Labelformulier
QC-formulier	DeelPIA/GEB
Code	WMK-toets
Mailwisselingen	4-ogen code review
	Testresultaten
	Aanvraag data/werk/productiegebied
	Beheer-/exploitatiehandleiding

Stap 4

Zodra ontwikkeling is afgerond, stuurt de analist een mail naar Toeslagen AU Quality Control Postbus met daarin het ingevulde QC-formulier en een concept rapportage of begeleidend document op scope en resultaten. Verstuur hierbij **geen** bestanden met herleidbare persoonsgegevens.

Stap 5

Vanuit de Toeslagen AU Quality Control Postbus krijgt de analist te horen of er een opdracht is geselecteerd voor QC: self-assessment mails verstuurd vóór 08.30 uur krijgen dezelfde werkdag vóór 12:00 uur een reactie. Mails verstuurd na 08:30 uur krijgen de volgende werkdag vóór 12:00 uur een reactie. Houd rekening met een gemiddelde doorlooptijd van een extra week als de opdracht voor QC in aanmerking komt.

Indien geselecteerd, dan kan de analist in het geval van Eenmalige Analyses of een Gegevensproduct zelf een tijdslot inplannen. Klik [hier](#) voor een actueel overzicht van de tijdsloten en hoe deze zijn in te plannen. Bij Rapportages & Dashboards, en Signaal- en Risicomodellen wordt het verzoek doorgezet door kwaliteitszorg naar QC'ers om een QC afspraak in te plannen. Klik hier voor meer informatie over het QC vrijgaveproces.

Bij spoed wordt ad-hoc een kwaliteitscontrole ingepland.

Opdrachten die op de DF&A tenant worden ontwikkeld (een DF&A werkgebied) worden volledig door de flexibele schil van DF&A uitgevoerd en volgen het QC traject van DF&A.

Stap 6

Wanneer het QC vrijgaveproces goed is doorlopen, kan er worden uitgeleverd. Hierbij lever je als analist het eindresultaat op aan je opdrachtgever. Let hier op de standaarden voor uitleveren en veilig versturen (T-31). Wanneer de analist de opdracht heeft uitgeleverd, zet hij of zij deze TSPM epic in de fase 'Done'.

Stap 7

Als het bij de uitgeleverde opdracht gaat om een product dat in exploitatie/beheer wordt genomen (zie definitie exploitatie/beheer) dan wordt er van de analist verwacht dat dit product wordt geregistreerd als (business) epic op het Toeslagen Exploitatie Board (TSEX). Binnen dit Jira project vindt men een handleiding wat en hoe er geregistreerd moet worden.

Alle verdere opdrachten en aanvragen kunnen dan gelinkt worden aan het TSEX epic.



Maatregelen
nemen

Privacybewustwording

Doelbinding

Noodzaak

Effecten in kaart

PIA
Bescherming van
persoonsgegevens

Risico's

minimaliseren

Richtinggevend

Rechtsgrond

Met open vizier