

Bijlagen bij brief van 9 juli 2025 met kenmerk 2025-002145

Bijlage 1: Bevindingen en conclusies RAM	2
Leeswijzer	2
Inleiding	2
Bevindingen uitgaande van het rapport van KPMG	2
Conclusies: in strijd met de Wet persoonsregistraties en de Wet bescherming persoonsgegevens	4
 Bijlage 2: Bevindingen en conclusies ‘met RAM vergelijkbare systemen’	7
Leeswijzer	7
1. Informatiesjabloon	8
Bevindingen en conclusies	8
Opdrachten aan de Belastingdienst	10
2. Klantbeeld Toezicht Applicatie (KTA)	12
Bevindingen en conclusies	12
Opdrachten aan de Belastingdienst	13
3. Gruff	14
Bevindingen en conclusies	14
Opdrachten aan de Belastingdienst	15
4. Invorderings Hulp Programma (IHP)	16
Bevindingen en conclusies	16
Opdrachten aan de Belastingdienst	17
5. Inforay Selectie Module OB (SMOB)	18
Bevindingen en conclusies	18
Opdrachten aan de Belastingdienst	19
6. Profiel-gebaseerd RISico Management (PRISMA)	20
Bevindingen en conclusies	20
Opdrachten aan de Douane	21

Bijlage 1: Bevindingen en conclusies RAM

Leeswijzer

Deze bijlage geeft eerst een samenvatting van de bevindingen die zijn opgenomen in het rapport van KPMG.¹ Daarna volgt een opsomming van de belangrijkste overtredingen van de Wet persoonsregistraties en de Wet bescherming persoonsgegevens.

Inleiding

De verwerkingen van persoonsgegevens met RAM hebben plaatsgevonden in de jaren 1998 tot 25 mei 2018. De eerste periode tot 1 september 2001 gold de Wet persoonsregistraties (WPR) en de periode vanaf deze datum tot 25 mei 2018 was de Wet bescherming persoonsgegevens (Wbp) van kracht. Beide wetten waren destijds van toepassing op de verwerkingen van persoonsgegevens door de Belastingdienst.²

De WPR bevatte al regels over het verzamelen en vastleggen van persoonsgegevens, toegang tot die gegevens en rechten van betrokkenen. Ook bevatte deze wet de plicht voor instanties om persoonsregistraties te melden bij de Registratiekamer (de voorloper van de AP). De WPR werd opgevolgd door de Wbp. Veel van de regels in de huidige AVG stonden ook in de Wbp. Zo bevatte de Wbp al de verschillende beginselen waaraan de gegevensverwerking moest voldoen³. Ook bevatte de Wbp regels over de specifieke bescherming voor bijzondere persoonsgegevens, de rechten van betrokkenen en de plicht tot het melden van een verwerking van persoonsgegevens bij de functionaris voor de gegevensbescherming (FG) en het College bescherming persoonsgegevens (Cbp), de voorganger van de AP.

Bevindingen uitgaande van het rapport van KPMG

Functionaliteit

RAM bood aan gebruikers twee functies: (1) het aan de hand van criteria selecteren van burgers/bedrijven en het oproepen van hun gegevens, en (2) het exporteren van deze gegevens in Excel. RAM had vrije, niet vooraf gedefinieerde, analysemogelijkheden.

Gegevens

In RAM werden zeer veel fiscale en niet-fiscale gegevens over burgers, fiscale dienstverleners en bedrijven samengebracht en na selectie op individueel of bedrijfsniveau raadpleegbaar en exporteerbaar gemaakt. Het ging onder andere om financiële gegevens gerelateerd aan bijna alle belastingmiddelen, aftrekposten zorgkosten, persoonlijke en bedrijfsrelaties, eerste- en tweede nationaliteit, schuldenpositie, KvK

¹ Kamerstukken II/2024/25, 31066, nr. 1465 en de bijlage: *Rapport onderzoek Risico Analyse Model (RAM) bij Belastingdienst, Dienst Toeslagen en Douane*, KPMG Accountants N.V., 7 februari 2025.

² Artikel 17 WPR en artikel 2-4 Wbp. Douane en de FIOD zijn gedurende de gehele periode onderdeel geweest van de Belastingdienst. Voor Toeslagen was dit vanaf 2005.

³ Rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid.

gegevens, Kadaster, WOZ, gegevens gerelateerd aan ontvangen toeslagen, gegevens over aftrekbare giften aan geloofsgenootschappen, gegevens over in- en uitvoer van goederen, autogegevens, en straf- en bestuursrechtelijke en fraudegegevens uit onder andere FSV. Het betrof gegevens verzameld door de Belastingdienst, door Dienst Toeslagen, de Douane en de FIOD.

Gebruikmakend van de samengebrachte brongegevens berekende RAM standaard ook totalen, percentages en scores per burger, adres, fiscaal dienstverlener of bedrijf. Bijvoorbeeld het aantal keren dat iemand in FSV stond, het aantal personen van een bepaalde nationaliteit⁴ per adres per jaar, het percentage aangifteverzuimen van een fiscaal dienstverlener, de verhouding veel/weinig winst uit omzet ten opzichte van soortgelijke ondernemingen etc.

Gebruik

RAM is gedurende 20 jaar intensief gebruikt binnen alle (toenmalige) onderdelen van de Belastingdienst⁵, door de FIOD, de Dienst Toeslagen en de Douane. RAM werd gebruikt voor toezicht en handhaving, opsporing en diverse andere werkzaamheden. Voorbeelden zijn: het opstellen van nalevingsbeelden, fraudedetectie, fenomeenanalyse, specifieke toezichtsprojecten op fiscaal en niet-fiscaal gebied (e.g. tegengaan witwassen, aanpak fiscaal dienstverleners), verrijking van signalen van niet-naleving van belastingwetgeving en de voorbereiding op boekenonderzoek. De werkzaamheden waren niet beperkt tot bepaalde belastingmiddelen. Ook werd RAM gebruikt om inzicht krijgen in de omvang van een probleem, de effectmeting van handhavingsinstrumenten en voor gegevensdeling met andere organisaties in het justitiële en sociale domein (al dan niet in het kader van een samenwerkingsverband).

Impact

Van hoeveel burgers en bedrijven er via RAM persoonsgegevens zijn geselecteerd, geëxporteerd en verder verwerkt in het kader van toezicht is helaas niet te vast te stellen. Wel volgt uit documenten dat in 2014 circa 35.000, in 2016 circa 22.000 en in 2017 21.394 keer in RAM er een bepaalde selectie van burgers en/of bedrijven is gemaakt en het resultaat (de gegevens van de geselecteerde burgers en bedrijven) is geëxporteerd in Excel. Dit kon leiden tot een Excel met de gegevens van één persoon of van duizenden. Grof geschat komt het totaal aantal selecties via RAM in de 20 jaar dat het systeem is gebruikt uit op een half miljoen.⁶

Gebrekkige vastleggen resultaten gebruik RAM

KPMG heeft geconcludeerd dat het gedurende de jaren dat RAM is gebruikt het ontbreken aan structurele vastlegging van hoe RAM ten aanzien van een burgers of bedrijf was ingezet en waartoe het concreet had geleid.

⁴ Afghaans, Bosnisch, Bulgaars, Colombiaans, Egyptisch, Ghanees, Hongaars, Iraakees, Iranee, Marokkaans, Nederlands, Nigeriaans, Pools, Roemeens, Surinaams, Tunesisch, Turks, Rest van Afrika, Australië en Oceanië, rest van Azië, rest van Europa, Noord-Amerika, rest van Zuid-Amerika.

⁵ Waaronder Particulieren, MKB en Grote ondernemingen.

⁶ Ongeveer 20 jaar vermenigvuldigd met het gemiddelde van (35.000, 22.000, 21.394) ≈ 523.000

Beveiliging

RAM was een applicatie die door medewerkers op de werkvloer is ontwikkeld en gaandeweg landelijk is uitgerold. RAM was dus een lokaal ontwikkelde applicatie (LOA) en niet een applicatie die conform minimale beveiligingsstandaarden door de ICT directie was ontwikkeld. Gebruikers met toegangsautorisaties tot RAM konden zelf de selectiecriteria kiezen en selecties maken, gebruikmakend van de in RAM opgenomen gegevens. KPMG heeft geen voorschriften of richtlijnen aangetroffen die het gebruik van selectiecriteria inkaderde, bijvoorbeeld het gebruik van gevoelige criteria zoals nationaliteit of strafrechtelijke gegevens.

Het aantal geautoriseerde gebruikers van RAM steeg van enkele medewerkers tot circa 250 in 2017. Alle Belastingdienstmedewerkers betrokken bij het houden van toezicht konden gegevensselecties bij deze geautoriseerde RAM-gebruikers aanvragen. De aangevraagde RAM-extracties werden met de aanvragers gedeeld door middel van naar Microsoft Excel geëxporteerde bestanden. De extracties waren niet standaard van beveiliging voorzien en konden onderling via e-mail of een USB-stick tussen medewerkers worden uitgewisseld en op de eigen computer of netwerkschijven worden opgeslagen.

Conclusies: in strijd met de Wet persoonsregistraties en de Wet bescherming persoonsgegevens

1. Onrechtmatige verwerking van (bijzondere en strafrechtelijke) persoonsgegevens

Artikel 18 WRP en, later, artikel 8 Wbp vereiste dat de Belastingdienst alleen persoonsgegevens mocht verwerken indien dit *noodzakelijk* was voor een goede invulling van diens publieke taak. De AP concludeert dat de verwerking onrechtmatig was aangezien niet was voldaan aan het noodzakelijkheidvereiste. De verwerking van persoonsgegevens middels RAM en daarna in de RAM-extracten was niet proportioneel.

Er is een onevenredige inbreuk gemaakt op de belangen van burgers en ondernemers in verhouding tot de met de verwerking te dienen doelen. Burgers en ondernemers werden gedurende een periode van 20 jaar geselecteerd op basis van allerlei gegevens, waaronder eerste en tweede nationaliteit, postcode en strafrechtelijke gegevens. Er waren nauwelijks beperkende maatregelen in RAM getroffen om de inbreuk op de persoonlijke levenssfeer te verkleinen. Veel gevoelige gegevens werden samengebracht, selecties konden vrij worden gemaakt en geautoriseerde medewerkers hadden inzicht in ‘alles op alles’.⁷ Het exporteren in Excel maakte dat de gegevens van geselecteerde personen buiten RAM beschikbaar kwamen.

De doelen waarvoor RAM werd gebruikt waren bovendien niet welbepaald. Ze liepen uiteen van opsporing tot bedrijfsvoering. De gevolgen voor burgers en ondernemers van het gebruik van RAM voor toezicht en opsporing zijn niet concreet vast te stellen maar dat het, al dan niet na een boekenonderzoek, heeft geleid tot financiële consequenties is zo goed als zeker. RAM werd namelijk binnen de Belastingdienst jarenlang beschouwd als een effectief middel om haar belastingopbrengsten te verhogen. Uit de door KPMG aangetroffen RAM-extracten blijkt bovendien dat veel van deze documenten te lang zijn bewaard, hetgeen bijdraagt aan de ernst van de inbreuk.

⁷ Paragraaf 14 van de gegevensbeschermingseffectbeoordeling RAM v1.0, bijlage bij *Kamerstukken II/2022/23*, 31066, nr. 1276.

In de gegevensbeschermingseffectbeoordeling (GEB) van RAM uit 2017 is door de Belastingdienst overigens ook zelf geconcludeerd dat op dat moment de verwerkingen van persoonsgegevens in RAM niet proportioneel waren.⁸

2. Discriminerende verwerkingen

Artikel 4 WRP en, later, artikel 6 Wbp vereiste dat de Belastingdienst alleen persoonsgegevens mocht verwerken voor zover (het doel) in overeenstemming was met de wet. Artikel 1 van de Grondwet, artikel 21 van het Handvest van de grondrechten van de Europese Unie en artikel 14 van het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) bevatten gedurende de periode dat RAM werd gebruikt het verbod op discriminatie.

RAM was een instrument om selecties van burgers en bedrijven te maken aan de hand van (vrije) criteria. Waar selecties worden gemaakt wordt onderscheid gemaakt en bestaat het risico op discriminatie. Het maken van onderscheid tussen personen was ook in die periode slechts toegestaan als hiervoor een objectieve rechtvaardigingsgrond bestond.

De AP concludeert dat er onderscheid is gemaakt tussen personen, waaronder op nationaliteit, en dat hiervoor tot op heden geen objectieve rechtvaardigingsgronden bekend zijn. Met RAM zijn, gelet hierop, discriminerende verwerkingen uitgevoerd. De volgende punten onderbouwen deze conclusie.

Ten eerste omdat er in RAM standaard een telling werd getoond van het aantal personen van alleen specifieke nationaliteiten per adres per jaar.⁹ Er zijn door KPMG geen documenten aangetroffen met de ratio achter deze telling; het is echter moeilijk voor te stellen dat hiervoor een objectieve rechtvaardiging was, die bovendien gedurende de hele looptijd van RAM opging.

Ten tweede omdat RAM is gebruikt om onderzoek te doen naar specifieke nationaliteiten waarbij, zo stelt het rapport van KPMG, werd *aangenomen* dat deze nationaliteiten eerder de regels zouden overtreden.¹⁰ Ook hiervoor is geen objectieve rechtvaardigingsgrond bekend.

Ten derde volgt uit de 14 aangetroffen RAM-extracten dat is geselecteerd op Bulgaarse, Roemeense, Afghaanse of Albanese nationaliteit als eerste en/of tweede nationaliteit. Ook voor deze selecties is geen objectieve rechtvaardiging aangetroffen. Hetzelfde gaat op voor de andere aangetroffen RAM-extracten waarbij selectiecriteria zijn gehanteerd waarvoor geen objectieve rechtvaardiging voor was, bijvoorbeeld postcode.¹¹

⁸ Paragraaf 14 van de gegevensbeschermingseffectbeoordeling RAM v1.0, bijlage bij *Kamerstukken II/2022/23*, 31066, nr. 1276.

⁹ Afghaans, Bosnisch, Bulgaars, Colombiaans, Egyptisch, Ghanees, Hongaars, Irakees, Iranes, Marokkaans, Nederlands, Nigeriaans, Pools, Roemeens, Surinaams, Tunesisch, Turks, Rest van Afrika, Australië en Oceanië, rest van Azië, rest van Europa, Noord-Amerika, rest van Zuid-Amerika.

¹⁰ Pagina 195 van *Rapport onderzoek Risico Analyse Model (RAM) bij Belastingdienst, Dienst Toeslagen en Douane*, KPMG Accountants N.V., 7 februari 2025.

¹¹ Er bestaat een lijst van gehanteerde veldnamen die als selectiecriteria zijn gebruikt, zie tabel 3.4.5.4.1 van het rapport KPMG voor de top 25. Een deel van de selectiecriteria blijft onduidelijk vanwege de cryptische naamgeving van de veldnamen.

3. Geen passende technische en organisatorische maatregelen getroffen

Artikel 8 WRP en, later, artikel 13 Wbp verplichtte de Belastingdienst om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen bijvoorbeeld tegen onbevoegde kennisneming, wijziging of verdere verwerking. De AP concludeert op basis van het onderzoek van KPMG dat de Belastingdienst onvoldoende maatregelen had getroffen om het systeem RAM en de RAM-extracten die daaruit voortkwamen te beveiligen.

Voor wat betreft de RAM-extracten geldt dat in het geheel geen sprake was van enige beveiliging. Zo waren de Excelsheets niet beveiligd met een wachtwoord en er waren geen voorschriften over het opslaan, kopiëren of delen van deze Excelsheets. Ten aanzien van het systeem RAM heeft KPMG vastgesteld dat er in beperkte mate beveiligingsmaatregelen waren getroffen die echter in belangrijke mate werden overgelaten aan de gebruikers van RAM. In 2017 is een interne beveiligingsanalyse van RAM uitgevoerd waarbij de bevindingen als 'critical' en 'high' werden gekwalificeerd. Er werd aanbevolen om de applicatie stil te leggen, hetgeen toen niet gedaan is.

4. Onttrokken aan het (toe)zicht

Op grond van artikel 19 WPR gold voor de Belastingdienst de verplichting om elke persoonsregistratie te melden aan de externe toezichthouder van toen, de Registratiekamer. Na inwerkingtreding van de Wbp werd de Belastingdienst verplicht om de reeds bestaande gegevensverwerkingen in RAM te melden bij het Cbp of de functionaris voor de gegevensbescherming.¹² KPMG heeft vastgesteld dat RAM niet was aangemeld bij de toezichthouder Cbp of de functionaris voor de gegevensbescherming. Hiermee handelde de Belastingdienst in strijd met de meldplicht. Dit heeft tot gevolg gehad dat de gegevensverwerkingen met RAM niet bekend waren bij de beide toezichthouders waardoor deze niet in staat zijn gesteld te acteren. Ook heeft dit tot gevolg gehad dat de verwerking *niet* in een voor een ieder te raadplegen register terecht zijn gekomen.¹³ Hierdoor was bij burgers en ondernemers, maar bijvoorbeeld ook de media, niet bekend welke verstreckende verwerkingen plaatsvonden bij de Belastingdienst.

¹² Artikel 27 jo. artikel 79 Wbp.

¹³ Artikel 28 Wbp.

Bijlage 2: Bevindingen en conclusies 'met RAM vergelijkbare systemen'

Leeswijzer

Deze bijlage behandelt elk van de zes systemen op dezelfde gestructureerde wijze. Voor elk systeem is achtereenvolgens het volgende beschreven.

Eerst wordt er een korte uitleg gegeven van de werking van het systeem, welke persoonsgegevens ermee worden verwerkt en voor welke doeleinden het wordt gebruikt. Om een indruk te geven van de omvang van de verwerking van persoonsgegevens met het systeem, wordt het aantal gebruikers van het systeem vermeld en, indien bekend, een schatting van het aantal personen wiens gegevens ermee zijn verwerkt in 2024.

Na de uitleg volgt een tabel met de bevindingen en conclusies van het onderzoek van de AP naar het systeem. De bevindingen zijn door middel van een kleur (groen, oranje, rood) gerangschikt naar mate van de ernst van de (mogelijke) overtreding van de AVG. De oranje en rode bevindingen benoemen daarnaast de AVG normen die in het geding zijn.

Tot slot is voor elk systeem een aantal opdrachten geformuleerd waarmee de systeemeigenaar, de Belastingdienst of de Douane, aan de slag moet.

1. Informatiesjabloon

Inschatting risico voor de bescherming van persoonsgegevens: **Hoog**

- In gebruik sinds 1999. Informatiesjabloon is een procedure voor medewerkers van de Belastingdienst om persoonsgegevens op te vragen en aangeleverd te krijgen in een Excel format met berekeningen, vrije tekstvelden en met macro's (genaamd Informatiesjabloon). Het Informatieloket Eindhoven van de Belastingdienst behandelt de aanvragen door de gegevens op te vragen in Apeldoorn en via e-mail te verstrekken aan de aanvragers.
- Gegevens van alle belastingplichtigen kunnen op deze manier worden opgevraagd, per BSN/RSIN¹⁴ of per postcode + huisnummer. De persoonsgegevens die kunnen worden opgevraagd: persoonlijke relaties (t/m 4de graad), loon- en uitkeringsgegevens, banksaldi, beleggingsgegevens, leengegevens, aangifte inkomstenbelasting, erf-schenkbelasting gegevens, vennootschapsbelasting gegevens, aangifte omzetbelasting gegevens, schulden, WOZ, renaissance, auto's, caravans, vaartuigen, ondernemingsrelaties, Kamer van Koophandel gegevens, geschiedenis ondernemingen, loonheffing, werkgevers en gegevens over ontvangen toeslagen. Gegevens tot 5 jaar terug.
- De verwerkingen met de persoonsgegevens zijn in ieder geval: opvragen, samenvoegen, categoriseren, gebruiken, aanvullen, muteren, opslaan en verwijderen.
- Doeleinden: Intern gebruik binnen Intensief Toezicht, o.a. controle van ondernemers en samenwerkingsverband RIEC. Daarnaast voor levering van gegevens aan andere overheden, waaronder OM en Politie.
- Aantal gebruikers: ongeveer 200 medewerkers vragen persoonsgegevens op via Informatiesjabloon, hoeveel medewerkers de ontvangen gegevens gebruiken is niet bekend.
- Aantal subjecten (personen en bedrijven samen) waarover in het jaar 2024 gegevens zijn geleverd voor intern gebruik: ca. 38.000. Voor doorlevering aan andere overheden: ca. 1.900.
- Vervanging? Er is een verzoek ('impuls') bij directie IV van de Belastingdienst ingediend voor de vervanging van Informatiesjabloon. Geen concrete planning.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
Elke aanvraag voor een gegevenslevering via Informatiesjabloon gaat langs een beoordelaar voor goedkeuring. Het is niet mogelijk om een aanvraag van jezelf goed te keuren.	-
Het gegeven Nationaliteit en strafrechtelijke gegevens kunnen niet worden opgevraagd via Informatiesjabloon.	-
In het aanvraagformulier staat dat gegevens over ontvangen toeslagen niet aan externen mogen worden geleverd.	-

¹⁴ Burger Service Nummer (BSN) en Rechtspersonen en Samenwerkingsverbanden Informatie Nummer (RSIN)

In handleidingen en op de intranetsite staat dat Informatiesjabloon niet mag worden gebruikt voor risicoselectie.	-
Een aanvraag om gegevens via Informatiesjabloon te verkrijgen kan in principe worden ingediend door alle medewerkers van de Belastingdienst. Dit kan leiden tot aanvragen vanuit personen die de gegevens niet nodig hebben of er niet zorgvuldig mee omgaan.	Grondslag ¹⁵ , minimale gegevensverwerking ¹⁶ , opslagbeperking ¹⁷
Aanvrager van gegevenslevering moet aanvraagvoorwaarden ondertekenen. Hier staat dat de aanvrager zich aan verschillende vereisten uit de AVG moet houden (o.a. proportionaliteit, subsidiariteit, bewaartermijnen, dataminimalisatie). De verantwoordelijkheid voor de naleving AVG wordt daarmee bijna volledig bij de medewerkers gelegd.	Grondslag, minimale gegevensverwerking, opslagbeperking
De procedure betreft een bewerkelijk proces van knippen-plakken en macro's. Er wordt door het Informatieloket Eindhoven wel een steekproef gedaan om te controleren of de juiste gegevens worden verstrekt aan de verschillende aanvragers. Er is aangegeven dat men geen signalen van aanvragers ontvangt dat verkeerde gegevens zijn aangeleverd.	Juistheid ¹⁸ , beveiliging
Via Informatiesjabloon zijn kentekens en adresgegevens op te vragen, dit zijn gewilde gegevens voor criminelen. Informatiesjabloon is wel betrokken bij het Programma Weerbaarheid Ondermijning Belastingdienst maar niet als 'hoog risico applicatie'.	Beveiliging
Het Informatiesjabloon kan (via macro's) een vermogensvergelijking maken, waarbij voor één adres de inkomsten en uitgaven worden geschat o.b.v. gegevens van de Belastingdienst, Toeslagen en algemene gegevens van het NIBUD. Dit betreft profilering waarvoor strengere transparantievereisten gelden.	Transparantie ¹⁹
In 2023 is een Privacy Impact Assessment van Informatiesjabloon uitgevoerd, waarbij er meerdere risico's zijn gesignaleerd. Deze PIA is echter een concept gebleven, er is geen FG advies gevraagd en er heeft geen besluitvorming plaatsgevonden. Wel zijn volgens de Belastingdienst de daarin genoemde mitigerende maatregelen genomen.	Verantwoordingsplicht ²⁰
Informatiesjabloon is een LOA (Lokaal Ontwikkelde Applicatie). Het beheer wordt niet gedaan door directie IV, welke bepaalde minimale beveiligingstandaarden hanteert. Daarnaast voldoet Excel niet aan belangrijke beveiligingseisen op het gebied van autorisatie en logging.	Beveiliging ²¹
Elke aanvraag voor gegevenslevering moet langs een beoordelaar. Goedkeuringsprocedure is niet adequaat, want (1) je kunt als aanvrager zelf de beoordelaar kiezen, (2) er is geen toetsingskader voor de	Grondslag,

¹⁵ Artikel 5 lid 1 onder a) AVG en artikel 6 AVG.

¹⁶ Artikel 5 lid 1 onder c) AVG.

¹⁷ Artikel 5 lid 1 onder e) AVG.

¹⁸ Artikel 5 lid 1 onder d) AVG.

¹⁹ Artikel 5 lid 1 onder a) AVG en artikelen 12-14 AVG.

²⁰ Artikel 5 lid 2 onder b) AVG.

²¹ Artikel 5 lid 1 onder f) AVG en artikel 32 AVG.

beoordelaar, (3) erg klein veld om reden aanvraag in te omschrijven, (4) geen vastlegging van reden aanvraag en resultaat beoordeling. Het is onduidelijk en oncontroleerbaar of de verwerking van persoonsgegevens na ontvangst ervan voldoet aan o.a. noodzakelijkheid/proportionaliteit/subsidiariteit.	minimale gegevensverwerking, verantwoordingsplicht
Door het combineren in Informatiesjabloon van verschillende gegevens wordt voor personen die getrouwd zijn of een geregistreerd partnerschap hebben indirect de seksuele gerichtheid zichtbaar. Deze kwalificeren daarmee als een bijzondere categorie van persoonsgegevens.	Uitzonderingsgrond bijzondere pg ²²
De BSN's/adressen waarvoor een goedgekeurde aanvraag is gedaan, blijven op meerdere plekken opgeslagen: in de mailboxen van de aanvragers en de beoordelaars, de postbus Informatieloket Eindhoven en op de netwerkschijf.	Minimale gegevensverwerking, opslagbeperking
Levering van (veel) gegevens in Excelformaat. De controle op de persoonsgegevens is kwijt na oplevering. Hoog risico op oneigenlijk gebruik.	Grondslag, minimale gegevensverwerking
Onduidelijk of levering en gebruik van persoonsgegevens van Toeslagen is toegestaan. Er is geen grondslagtoets aangetroffen.	Grondslag en Uitzonderingsgrond bijzondere pg
Onduidelijkheid over de precieze doeleinden waarvoor en binnen welke werkzaamheden de persoonsgegevens intern Belastingdienst worden gebruikt.	Doelbinding ²³ , grondslag, verantwoordingsplicht
Via Informatiesjabloon kan niet alleen geleverd worden op subnummer-niveau. Als alleen gegevens over huisnummer 8a nodig zijn, ontvangt de aanvrager ook de persoonsgegevens van de bewoners van 8b, 8c enz. De aanvrager moet deze zelf verwijderen.	Minimale gegevensverwerking
Er worden (d.m.v. Informatiesjabloon) te veel persoonsgegevens verstrekt aan Politie/OM en mogelijk ook andere overheden en samenwerkingsverbanden. Aan Politie/OM worden bovendien de gegevens aangeleverd in het Informatiesjabloon (de Excel met berekeningen en macro's) met kans op fouten en onjuiste interpretatie van de gegevens tot gevolg.	Grondslag, minimale gegevensverwerking, juistheid

Opdrachten aan de Belastingdienst

1. Kom uiterlijk 15 oktober 2025 met een concreet plan voor de vervanging van Informatiesjabloon op de korte termijn. Bepaal in overleg met de AP het moment van vervanging.
2. Rond het PIA traject dat in 2023 is gestart versneld af, betrek de FG daarbij en tref voor de periode dat Informatiesjabloon nog actief is de uit het PIA traject voortvloeiende mitigerende maatregelen. Informeer de AP hierover.

²² Artikel 5 lid 1 onder a) AVG en artikel 9 AVG.

²³ Artikel 5 lid 1 onder b) AVG.

3. Tref daarnaast zo snel als mogelijk de volgende noodzakelijke mitigerende maatregelen:
 - a. Ontwikkel en implementeer een nieuwe beoordelingsprocedure voor aanvragen om gegevens via Informatiesjabloon, zodat de verwerking van persoonsgegevens na levering zoveel als mogelijk voldoet aan de AVG.
 - b. Pas de aanvraagprocedure zo aan dat het opslaan op meerdere locaties van de aangevraagde persoonsgegevens wordt geminimaliseerd.
 - c. Breng in kaart voor welke doeleinden en werkzaamheden de opgevraagde persoonsgegevens intern worden gebruikt, toets op noodzakelijkheid/proportionaliteit/subsidiariteit en neem indien nodig maatregelen.
 - d. Bepaal of er een grondslag bestaat voor het leveren en gebruiken van de gegevens van Toeslagen, en neem indien nodig maatregelen.
 - e. Bouw waarborgen in dat de aanlevering aan Politie/OM, andere overheden en samenwerkingsverbanden is beperkt tot wat noodzakelijke is, en neem in acht dat ook bijzondere categorieën van persoonsgegevens worden verstrekt.
 - f. Laat het Loket Eindhoven de persoonsgegevens van burgers en bedrijven op de teveel geleverde subnummers verwijderen in plaats van de aanvragers.
 - g. Verwijder het gegeven kenteken.
4. Het systeem biedt de mogelijkheid om door het combineren van gegevens iemands seksuele gerichtheid af te leiden. Dit betreft een bijzondere categorie van persoonsgegevens die de Belastingdienst niet nodig heeft voor haar toezichttaak. Het is de AP overigens duidelijk dat de Belastingdienst niet de intentie heeft om seksuele gerichtheid te verwerken. Door de toenemende digitalisering zijn gegevens echter steeds sneller en eenvoudiger te koppelen. Dat maakt dat wat (bijzondere) persoonsgegevens zijn altijd moet worden beoordeeld in het licht van deze zich wijzigende context. Ook in de uitspraken van het Hof van Justitie van de Europese Unie over de reikwijdte van bijzondere categorieën van persoonsgegevens is dit terug te lezen.²⁴ Bijzondere categorieën van persoonsgegevens zijn naar hun aard bijzonder gevoelig en de verwerking kan significante risico's voor de rechten en vrijheden van personen met zich meebrengen. Gezien het voorgaande roept de AP de Belastingdienst op om het risico op het verwerken van seksuele voorkeur in de opvolger van Informatiesjabloon uit te sluiten, en dit onderdeel te maken van haar privacy-by-design.

²⁴ HvJ EU 1 augustus 2022, C-184/20 (*Vyriausioji tarnybinės etikos komisija*), HvJ EU 4 juli 2023 (*Meta Platforms e.a.*), HvJ EU 4 oktober 2024 (*Lindenapotheker*).

2. Klantbeeld Toezicht Applicatie (KTA)

Inschatting risico voor de bescherming van persoonsgegevens: **Hoog**

- In gebruik sinds 2013. KTA is een applicatie met schermen die voor één BSN of RSIN praktisch alle (persoons)gegevens die binnen de Belastingdienst beschikbaar zijn toont. Bevat ook berekeningen. Het is een basissysteem dat door veel medewerkers van de Belastingdienst dagelijks wordt gebruikt.
- Gegevens van alle belastingplichtigen kunnen op deze manier worden getoond (m.u.v. VIP-gegevens). De persoonsgegevens die worden getoond zijn o.a.: NAW, geslacht, relaties, geboortedatum, immigratiedatum, emigratiedatum, curator/bewindvoerder, bankgegevens, loongegevens, vastgoed, voertuigen, relevante gegevens aangaande alle belastingmiddelen, voorlopige en definitieve aanslagen, navorderingen, teruggaven, ontvangen betalingen, invorderingskosten. Behandelverslagen van controle en toezicht. Bezwaar/beroep-informatie. Gegevens over fiscale dienstverleners. Tot 5 jaar terug.
- De verwerkingen met de persoonsgegevens zijn in ieder geval: raadplegen, combineren, exporteren (alleen gegevens aangaande vennootschapsbelasting).
- Doeleinde: heffing, inning en toezicht.
- Aantal gebruikers van het systeem: 18.000 medewerkers van de Belastingdienst.
- Vervanging? Er wordt al een paar jaar niet meer geïnvesteerd in KTA, want het moet vervangen worden door andere applicatie. Nog geen planning bekend voor de overgang naar het nieuwe systeem.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
In beheer bij directie IV, geen LOA.	-
Het gegeven Nationaliteit en strafrechtelijke gegevens worden niet getoond in KTA.	-
In KTA worden alleen gegevens getoond (klantbeeld), geen risicoselectie.	-
De raadplegingen in KTA worden gelogd, actieve monitoring is nog niet geïmplementeerd (opzet is gereed).	Beveiliging
In KTA zijn kentekens en adresgegevens te raadplegen, dit zijn gewilde gegevens voor criminelen. KTA is betrokken bij het Programma Weerbaarheid Ondermijning Belastingdienst.	Beveiliging
Onduidelijk of medewerkers van Belastingdienst/Toeslagen, Douane en de FIOD via KTA de persoonsgegevens van de Belastingdienst mogen verwerken. Er is geen grondslagtoets aangetroffen.	Grondslag, doelbinding
Slechts 1 rol (los van autorisatie VIP-gegevens) voor alle medewerkers die toegang hebben, waardoor voor elk van deze medewerkers alle schermen met (persoons)gegevens ingezien kunnen worden. KTA wordt gebruikt voor uiteenlopende werkzaamheden binnen heffing, inning en toezicht.	Grondslag, minimale gegevensverwerking, doelbinding

Door het combineren in KTA van verschillende gegevens wordt voor personen die getrouwd zijn of een geregistreerd partnerschap hebben indirect de seksuele gerichtheid zichtbaar. Deze kwalificeren daarmee als een bijzondere categorie van persoonsgegevens.	Uitzonderingsgrond bijzondere pg
Gegevens in KTA over studiefinanciering, WOZ en vaartuigen zijn verouderd (uit 2021) en nog steeds te raadplegen.	Juistheid
Exportfunctionaliteit, weliswaar niet voor alle gegevens maar wel de gegevens van aanslagen en aangiftes. De controle op de persoonsgegevens is kwijt na exporteren. Ook wordt het gebruik van deze functionaliteit niet gelogd.	Beveiliging
Onduidelijkheid over de precieze doeleinden waarvoor KTA wordt gebruikt.	Doelbinding, grondslag, verantwoordingsplicht
Er zijn geen gegevensbeschermingseffectbeoordelingen van verwerkingen van persoonsgegevens waarbij KTA wordt ingezet overlegd.	Verantwoordingsplicht

Opdrachten aan de Belastingdienst

1. Kom uiterlijk 15 oktober 2025 met een concreet plan voor de vervanging van KTA op de korte termijn. Bepaal in overleg met de AP het moment van vervanging.
2. Tref daarnaast zo snel als mogelijk de volgende noodzakelijke mitigerende maatregelen:
 - a. Richt een strak proces in van actieve monitoring van de logging om alleen noodzakelijke verwerkingen van persoonsgegevens te waarborgen.
 - b. Onderzoek of medewerkers van Belastingdienst/Toeslagen, Douane en de FIOD via KTA persoonsgegevens, die zijn verzameld door de Belastingdienst, mogen verwerken. Neem indien nodig maatregelen.
 - c. Verwijder in KTA de verouderde gegevens over studiefinanciering, WOZ en vaartuigen.
 - d. Scherm kentekengegevens en adresgegevens af of vind een andere oplossing om de toegang tot deze gegevens te beperken/te monitoren.
3. Ten aanzien van de verwerking in KTA van gegevens betreffende seksuele gerichtheid, verwijst de AP naar de vierde opdracht ten aanzien van Informatiesjabloon.

3. Gruff

Inschatting risico voor de bescherming van persoonsgegevens: **Midden**

- In gebruik sinds 2014. Een tool om relaties die aanwezig zijn in data te visualiseren. Het betreft relaties tussen personen, bedrijven en objecten (e.g. auto, telefoonnummer).
- De persoonsgegevens waar Gruff gebruik van maakt komen uit basissystemen van de Belastingdienst: Beheer van Relaties, KvK, ANBI, Loon, Auto, Bank. De persoonsgegevens die met Gruff worden verwerkt zijn onder andere: BSN, NAW, geslacht, geboortedatum, huwelijk/geregistreerd partner, ouders, kinderen, ex-partner, bedrijfsinformatie, bestuurders, aandeelhouders, inkomstengegevens per jaar, werkgever, kenteken auto, datum gekocht/verkocht, bankrekeningen. Over een periode van 5 jaar terug.
- De verwerkingen met de persoonsgegevens zijn in ieder geval: combineren, raadplegen, exporteren, opslaan, gebruiken en wissen.
- Doeleinden: aanpak risicovolle netwerken, intensief toezicht binnen de directies MKB en GO, FIOD niet meer.
- Aantal gebruikers van het systeem: c.a. 60 medewerkers van de Belastingdienst, de met Gruff gemaakte visualisaties worden wel door meer medewerkers gebruikt.
- Schatting aantal personen wiens gegevens in 2024 zijn verwerkt: ca 13.500.²⁵
- Vervanging? Door directie DF&A is bepaald dat per september 2026 de data van Gruff niet meer wordt ververst waardoor het gebruik van Gruff stopt.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
Gebruikers van Gruff binnen de directie MKB moeten verplicht voorafgaand aan elke visualisatie in een tool vastleggen waarvoor ze Gruff gaan gebruiken.	-
Gebruikers van Gruff binnen directie GO moeten verplicht voorafgaand aan elke visualisatie in een formulier vastleggen waarvoor ze Gruff gaan gebruiken en waarom dit voldoet aan de AVG eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.	-
Maandelijkse lograpportages per gebruiker welke personen zijn 'geraakt' in een visualisatie.	-
Grondige risicoanalyse uitgevoerd in 2022/2023, wat heeft geleid tot een reeks mitigerende maatregelen.	-
Geen gegeven nationaliteit en geen strafrechtelijke gegevens.	-
Extern ingekochte tooling. Beheer door directie DF&A, niet door directie IV. Wel is gesteld dat de meeste IV-standaarden worden nageleefd.	Beveiliging

²⁵ Inschatting gebaseerd op de rapportage logging van directie DF&A over februari 2025.

Elke gebruiker van Gruff moet verplicht akkoord gaan met de voorwaarden van directie DF&A. Hier staat o.a. in dat Gruff alleen gebruik mag worden voor toezicht, doelbinding, gebruik proportioneel moet zijn en dat de data niet mag worden geëxporteerd. De verantwoordelijkheid voor de naleving AVG wordt daarmee bijna volledig bij de medewerkers gelegd.	Grondslag, minimale gegevensverwerking, opslagbeperking
Gruff toont hoogte van loon/uitkering/inkomsten uit andere betrekkingen, onduidelijk waarom dit noodzakelijk is voor een netwerkanalyse.	Minimale gegevensverwerking
De visualisatie is in een plaatje te exporteren. De achterliggende data is te exporteren in xlm (niet een gebruiksvriendelijk format).	Beveiliging
Beperkt aantal autorisaties tot Gruff maar meer medewerkers gebruiken de visualisaties in hun werk.	Grondslag, minimale gegevensverwerking
Door het combineren in Gruff van verschillende gegevens wordt voor personen die getrouwd zijn of een geregistreerd partnerschap hebben indirect de seksuele gerichtheid zichtbaar. Deze kwalificeren daarmee als een bijzondere categorie van persoonsgegevens.	Uitzonderingsgrond bijzondere pg
Gebruikers ervaren geregeld fouten in de gegevens die worden gebruikt door Gruff. Deze fouten zitten in de onderliggende bronsystemen. Deze bronsystemen worden ook door andere systemen gebruikt.	Juistheid
Onduidelijkheid over de precieze doeleinden waarvoor en werkzaamheden waarbinnen Gruff wordt gebruikt (m.u.v. team ARN)	Verantwoordingsplicht
Slechts twee personen binnen DF&A die Gruff kunnen beheren.	Beveiliging
Exporteren wordt niet gelogd.	Beveiliging
Niet is gebleken dat de directies MKB en GO, opvolgend op DF&A, een DPIA hebben uitgevoerd, waardoor onduidelijk is of de recent doorgevoerde maatregelen de risico's voldoende mitigeren. Ook is de FG hierdoor niet betrokken.	Verantwoordingsplicht
Gruff-analyses worden tijdelijk opgeslagen op de Q-schijf en na een paar weken verwijderd. Onduidelijk hoe dit zich verhoudt tot de Archiefwet.	Beveiliging

Opdrachten aan de Belastingdienst

1. Stop conform de planning met het gebruik van Gruff per september 2026.
2. Tot die tijd, tref zo snel als mogelijk de volgende noodzakelijke mitigerende maatregelen:
 - a. Onderzoek of de hoogte van inkomsten noodzakelijk is voor de verwerking van persoonsgegevens en tref indien nodig maatregelen.
 - b. Onderzoek of het wissen van de Gruff visualisaties in lijn is met de Archiefwet en tref indien nodig maatregelen.
3. Ten aanzien van de verwerking in Gruff van gegevens betreffende seksuele gerichtheid, verwijst de AP naar de vierde opdracht ten aanzien van Informatiesjabloon.

4. Invorderings Hulp Programma (IHP)

Inschatting risico voor de bescherming van persoonsgegevens: **Laag**

- In gebruik sinds 2005. Applicatie heeft meerdere functies met betrekking tot inning, o.a. het geven van een overzicht per BSN/RSNIN van de openstaande belastingschulden, het verzenden van dit overzicht per brief aan belastingplichtige of derde en het corrigeren van foutieve kosten- en rentevaststellingen.
- In de applicatie staan gegevens van een specifieke groep belastingplichtigen (burgers en bedrijven), namelijk diegenen die een dwangbevel hebben gekregen omdat zij niet tijdig een belastingsschuld hebben betaald en diegenen met een bijzondere vordering (e.g. minnelijke schuldsanering).
- De verwerkingen met de persoonsgegevens zijn in ieder geval: raadplegen, genereren van brieven, muteren.
- Doelinden: invordering en dienstverlening.
- Aantal gebruikers van het systeem: c.a. 2.000 medewerkers van de Belastingdienst.
- Vervanging? Een deel van de functionaliteit is inmiddels overgenomen door andere applicaties die door directie IV worden beheerd. Er ligt een ontmantelingsplan wat stelt dat tweede kwartaal 2026 de applicatie grotendeels moet zijn ontmanteld.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
Toegang tot persoonsgegevens is beperkt tot de regio en afhankelijk van autorisatierol.	-
Op startscherm staat de datum waarop de data voor het laatst is ververs.	-
Geen gegeven nationaliteit, geen bijzondere categorieën van persoonsgegevens, geen strafrechtelijke gegevens.	-
Opmaken en exporteren van een schuldenoverzicht (in een brief) wordt gelogd.	
Het IT landschap rond de applicatie is complex, met verscheidene bronsystemen, gegevensstromen, verschillende verversmomenten, exportprocessen, meerdere afnemers enz.	Beveiliging, juistheid
Een deel van de functionaliteit van IHP is overgegaan op andere applicaties, maar is in IHP nog wel benaderbaar.	Beveiliging, juistheid
Het is mogelijk om een schuldenoverzicht per post naar een onbevoegde te sturen door het adres handmatig aan te passen.	Beveiliging
Geen kentekengegevens. Wel adresgegevens, dit zijn gewilde gegevens voor criminelen.	Beveiliging
IHP is een LOA met kritische functionaliteit.	Beveiliging
In 2026 pensionering van de enige functioneel beheerder.	Beveiliging

IHP toont gegevens over invorderingsschulden van Toeslagen, onduidelijk of hiervoor een grondslag is.	Grondslag
Binnen de processen Innen en Betalen die gebruikmaken van IHP worden bewaartermijnen niet nageleefd	Opslagbeperking

Opdrachten aan de Belastingdienst

1. Accepteer geen nieuwe functionaliteitswensen meer in IHP, voer het opgestelde ontmantelingsplan conform planning uit en stopt grotendeels met IHP in het tweede kwartaal van 2026.
2. Tot die tijd, tref de volgende noodzakelijke mitigerende maatregelen:
 - a. Onderzoek of er een grondslag is voor het verwerken van invorderingsschulden van Belastingdienst/Toeslagen en tref indien nodig maatregelen.
 - b. Neem de noodzakelijke stappen om te bewerkstellingen dat binnen de processen Innen en Betalen de vastgestelde bewaartermijnen worden gerespecteerd.

5. Inforay Selectie Module OB (SMOB)

Inschatting risico voor de bescherming van persoonsgegevens: **Laag**

- In gebruik sinds 2001. Met SMOB kunnen omzetbelasting-gegevens worden geraadpleegd (klantbeeld) door te zoeken op het OB-nummer of dossiernummer. Voorheen werd SMOB ook gebruikt voor het controleren van bedrijven op 'trefferslijsten' (ondernemingen die waren geselecteerd voor controle).
- De persoonsgegevens die kunnen worden geraadpleegd in SMOB zijn onder andere: algemene gegevens (NAW, fiscaal nummer, branche, openstaande schuld), binnenlandse en buitenlandse omzetbelasting-specifieke gegevens, zoals omzetgegevens goederen/diensten per EU-lidstaat, intracommunautaire transacties, opgave ICP, L1F1 formulier, openstaande schulden.
- De verwerkingen met de persoonsgegevens zijn in ieder geval: combineren, raadplegen, gebruiken.
- Doelinden: toezicht, voornamelijk controle opgaaf intracommunautaire prestaties (ICP) en behandelen signalen carousselfraude.
- Aantal gebruikers van het systeem: c.a. 2.300 medewerkers van de Belastingdienst.
- Vervanging? Het aanbestedingstraject voor de pakketoplossing voor OB als geheel is afgerond, dit zal SMOB in ieder geval gaan vervangen. Streven is 2027 in productie. Eerder al zal de applicatie Inzicht zorgen voor vervanging van SMOB.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
SMOB wordt niet gebruikt voor risicoselectie, alleen klantbeeld.	-
SMOB toont alleen bedrijfsgegevens, welke echter wel persoonsgegevens zijn in geval van eenmanszaken en zzp-ers. Er worden geen gegevens over bestuurders van bedrijven getoond. SMOB bevat ook geen gegevens meer vanuit de Douane.	-
Geen gegeven nationaliteit, geen bijzondere categorieën van persoonsgegevens, geen strafrechtelijke gegevens	-
Resultaten van het gebruik van SMOB worden vastgelegd in het klantdossier.	-
De verwerking in SMOB is noodzakelijk omdat alleen hier de intracommunautaire prestaties van bedrijven worden getoond, wat niet in andere applicaties raadpleegbaar is.	-
SMOB is een LOA, het beheer wordt wel gedaan door directie IV.	Beveiliging
Een deel van de functionaliteit van SMOB wordt niet meer gebruikt, maar is nog wel benaderbaar. Dit bevat soms verouderde gegevens.	Beveiliging, juistheid, opslagbeperking

Alle gegevens uit SMOB kunnen worden geëxporteerd in Excel door rol raadpleger. Lijkt echter niet te worden gebruikt. Ook mogelijk export in Word en PDF.	Beveiliging
SMOB toont openstaande fiscale boetes, onduidelijk waarom dit relevant is.	Minimale gegevensverwerking
Op korte termijn pensionering van de enige technisch beheerder van SMOB.	Beveiliging
Onduidelijkheid over welke directie van de Belastingdienst verantwoordelijk is voor SMOB en voor welke doeleinden en werkprocessen SMOB wordt gebruikt	Verantwoordingsplicht

Opdrachten aan de Belastingdienst

1. Vervang SMOB conform planning door de pakketoplossing voor de OB-keten of de applicatie Inzicht en zorg ervoor dat dit voldoende prioriteit behoudt zodat het gebruik van SMOB in 2027 of eerder stopt.
2. Tot die tijd, tref de volgende noodzakelijke mitigerende maatregelen:
 - a. Maak de functionaliteit die niet meer wordt gebruikt ontoegankelijk voor medewerkers en verwijder eventueel hier opgeslagen verouderde gegevens.
 - b. Breng in kaart voor welke doeleinden en werkzaamheden SMOB wordt gebruikt, toets op noodzakelijkheid/proportionaliteit/subsidiariteit en tref indien nodig maatregelen.
 - c. Onderzoek of de gegevens over openstaande fiscale boetes noodzakelijk is voor de verwerking van persoonsgegevens en tref indien nodig maatregelen.
 - d. Bepaal de verantwoordelijke directie en leg dit vast.

6. Profiel-gebaseerd RISico Management (PRISMA)

Inschatting risico voor de bescherming van persoonsgegevens: **Laag**

- In gebruik sinds 2005. PRISMA is niet één applicatie maar een landschap aan applicaties en databases. Er zijn risicoprofielen in opgeslagen en aan de hand van aangiftegegevens en contra-informatie wordt bepaald welke goederen wel en niet worden gecontroleerd (fysieke controle en/of bescheidscontrole).
- De persoonsgegevens die PRISMA gebruikt om risicoselecties te maken: bedrijfsgegevens afkomstig van goederenaangiften en o.a. gegevens van de Kamer van Koophandel. De aangiftegegevens die de Douane ontvangt staan genoemd in het Douanewetboek van de Unie.
- De verwerkingen van de persoonsgegevens zijn in ieder geval: verzamelen, combineren, gebruiken, verwijderen.
- Doeleinden: Toezicht op het EU buitengrens-overschrijdende goederenverkeer (invoer, uitvoer, binnenbrengen en uitgaan).
- Aantal gebruikers van het systeem: c.a. 40 medewerkers van de Douane.
- Vervanging? Niet voorzien.

Bevindingen en conclusies

Omschrijving	AVG norm in geding
PRISMA gebruikt alleen bedrijfsgegevens, welke echter wel persoonsgegevens zijn in geval van eenmanszaken en zzp-ers.	-
Geen gegeven nationaliteit, geen bijzondere categorieën van persoonsgegevens, geen strafrechtelijke gegevens.	-
Geen kentekens en adresgegevens in PRISMA.	-
Onduidelijkheid over het percentage eenmanszaken en zzp-ers waardoor onbekend is wat de omvang van de verwerking van persoonsgegevens is en of er mogelijk toch een DPIA moet worden uitgevoerd.	Verantwoordingsplicht
Voor niet alle gevallen is er na selectie in PRISMA sprake van de fase van 'het geoefend oog' en dus van menselijke tussenkomst. Hier lijkt sprake van geautomatiseerde besluitvorming. Onduidelijk is of er wordt voldaan aan artikel 22 AVG.	Geautomatiseerde besluitvorming
Er is sprake van profilering van personen (eenmanszaken en zzp-ers) en mogelijk ook van geautomatiseerde besluitvorming, waarvoor strengere transparantievereisten gelden.	Transparantie

Opdrachten aan de Douane

Tref zo snel als mogelijk de volgende noodzakelijke mitigerende maatregelen:

1. Ga na of er wordt voldaan aan de transparantievereisten voor wat betreft de verwerkingen van persoonsgegevens in PRISMA, en tref indien nodig maatregelen.
2. Ga na of er voor wat betreft PRISMA wordt voldaan aan de vereisten in artikel 22 AVG, betrek hierbij het advies van de AP,²⁶ en tref indien nodig maatregelen.
3. Inventariseer welk deel van de bedrijven waarvan gegevens worden verwerkt in PRISMA eenmanszaken en zzp-ers betreft en bepaal of er niet alsnog een DPIA nodig is.

²⁶ Advies artikel 22 AVG en geautomatiseerde selectie-instrumenten d.d. 10 oktober 2024 met kenmerk 2024-011279.