Privacy impact assessment m.b.t. de wijziging van de Vreemdelingenwet 2000

in verband met de uitbreiding van het gebruik van biometrische kenmerken in de vreemdelingenketen in verband met het verbeteren van de identiteitsvaststelling van de vreemdeling

1. Inleiding

Met het wetsvoorstel voor het gebruik van biometrische kenmerken in de vreemdelingenketen wordt het huidige gebruik van biometrische gegevens uitgebreid tot alle vreemdelingen en voor alle processen binnen de vreemdelingenketen voor de vaststelling en verificatie van de identiteit van de vreemdeling met het oog op de uitvoering van de Vreemdelingenwet 2000. Voorgesteld wordt om hiervoor gebruik te maken van een gezichtsopname en tien vingerafdrukken als biometrische identificatiemiddelen[1]. Voorts voorziet het wetsvoorstel in een juridische basis voor de opslag in een centraal gegevensbestand van de biometrische gegevens van vreemdelingen. Het wetsvoorstel maakt een grootschalige verwerking van persoonsgegevens mogelijk.

In de motie Franken c.s.[2] is bepaald dat bij nieuwe wetgeving waarin een dergelijke verwerking wordt voorgesteld uitdrukkelijk aandacht moet worden besteed aan de vraag of de beperkingen op het grondrecht tot bescherming van de persoonlijke levenssfeer gerechtvaardigd zijn. Deze motie past binnen de trend dat privacy in toenemende mate in maatschappelijke en politieke belangstelling staat. De exponentiële groei van het aantal informatiesystemen, het gemak waarmee deze aan elkaar kunnen worden gekoppeld en de mogelijkheden om deze systemen te doorzoeken zijn hier debet aan.
Ten behoeve van uitwerking van nieuwe wetgeving wordt daarom een privacy impact assessment (PIA) uitgevoerd om vooraf te onderzoeken welke risico's de voorgestelde maatregelen met zich meebrengen en op welke wijze deze risico's kunnen worden ondervangen. In de kabinetsreactie op het WRR rapport "iOverheid: de rol van de overheid in de iSamenleving" is dit assessment bij de Tweede Kamer aangekondigd.[3]

[1] Het gaat hier om een verwerking van persoonsgegevens in de zin van artikel 1 sub a van de Wet bescherming persoonsgegevens (vingerafdrukken) en om verwerking van bijzondere persoonsgegevens in de zin van artikel 16 van de Wet bescherming persoonsgegevens (gelaatsopname).
[2] Kamerstukken I 2010/11, 31 051, nr. D, Kabinetsbrief over privacy, Kamerstuk 32 761 en de aanwijzing 162a en 162b van de Aanwijzingen voor de regelgeving.
[3] Kamerstuk 2011-2012, 26 643 nr. 211.

2. Opzet privacy impact assessment

Voor het uitvoeren van een PIA is nog geen Nederlands standaardmodel voorhanden. In eerste instantie is voor de PIA het in het Verenigd Koninkrijk ontwikkelde toetsmodel gehanteerd.[4] Dit toetsmodel is het enige model dat is toegesneden op de Europese privacyrichtlijn die op dit wetsvoorstel van toepassing is. Het toetsmodel bestaat uit vragen die samenhangen met de universele beginselen van gegevensbescherming: rechtmatige grondslag, doelbinding, toereikendheid en gegevensminimalisering, juist en nauwkeurig, beperkt bewaren, rechten van betrokkenen, gegevensbeveiliging en gegevensverkeer met derde landen. Door het analyseren van de antwoorden op de vragen die samenhangen met de bovenstaande beginselen werd inzichtelijk hoe de bepalingen van dit wetsvoorstel zich verhouden tot het recht op bescherming van de persoonlijke levenssfeer en genoemde beginselen in het bijzonder.

Het PIA is uitgevoerd door de directie Identiteitsmanagement en Immigratie van het ministerie van BZK. In het Tactisch regieoverleg biometrie in de vreemdelingenketen, waarin alle ketenpartners vertegenwoordigd zijn, zijn de bevindingen van de PIA getoetst bij de ketenpartners met kennis over de uitvoeringspraktijk.

Uitgangspunten bij het PIA zijn geweest het doel waarvoor de gegevens mogen worden verwerkt zoals bepaald in het wetsvoorstel en de in het wetsvoorstel genoemde bewaartermijn van de gegevens.
In het PIA zijn de risico's van het afnemen van de biometrische gegevens, de opslag van de gegevens, het gebruik en de wijziging van gegevens, de verstrekking aan derden en de vernietiging van de gegevens in beeld gebracht.

De beoordeling betreft alleen de maatregelen die uit het wetsvoorstel voortvloeien. De maatregelen die worden doorgevoerd op grond van de verordeningen voor de biometrische gegevens op het vreemdelingendocument, voor de visa kort verblijf (EU-VIS) en voor asielzoekers in verband met Eurodac zijn niet meegenomen. Evenmin worden de ontwikkelingen meegenomen die uit wijzigingen in de regelgeving van de strafrechtsketen voortvloeien, zoals de WIVVG.
Bij het opstellen van het PIA is wel rekening gehouden met verplichtingen die voortvloeien uit Europese richtlijnen die ten tijde van de inwerkingtreding van dit wetsvoorstel gelden en met Opinion 3/2012 on developments in biometric technologies van de Artikel 29 Werkgroep.[5]

[4] The Information Commissioner's Office, Privacy Impact Assessment Handbook, version 2.0.

[5] Zie: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en en Opinion 3/2012 on developments in biometric technologies van De Artikel 29 Werkgroep, aangenomen op 27 april 2012, hoofdstuk 5.

3. Gebruik van biometrie binnen de vreemdelingenketen

Met dit wetsvoorstel wordt voorzien in de bevoegdheid om tien vingerafdrukken en een gezichtsopname af te nemen van alle vreemdelingen voor de identiteitsvastelling en verificatie ten behoeve van de uitvoering van de Vreemdelingenwet. Tevens wordt voorzien in de bevoegdheid om de gegevens centraal op te slaan in de vreemdelingenadministratie. De Basisvoorziening Vreemdelingen (BVV) is de database waarin de biometrische gegevens worden opgeslagen. De gegevens kunnen worden geraadpleegd voor de in het wetsvoorstel genoemde doelen. Dit kan door automatische bevraging van de BVV door een geautoriseerde ambtenaar. In het wetsvoorstel is een maximale bewaartermijn opgenomen voor de gegevens (tien jaar).

In onderstaande tabel wordt aangegeven:
1. in welke processen en door welke ketenorganisaties binnen de vreemdelingenketen al gebruik kan worden gemaakt van vingerafdrukken (X),
2. bij welke processen een uitbreiding van het gebruik door het wetsvoorstel mogelijk wordt gemaakt (U), en
3. bij welke processen de afname van tien vingerafdrukken door het wetsvoorstel mogelijk wordt gemaakt (N).

	BZ	KMar	(V)P	ZHP	IND	COA	DTeV	DJI
Inburgering	x							
Visum kort verblijf (EU VIS)	x	x		x	x			
Machtiging voorlopig verblijf	N				N			
Verblijfsvergunning regulier					N			
Verblijfsvergunning asiel		x	x		N			
Binnenlands toezicht		U	U	U				
Grensbewaking		U		U				
Terugkeer en Vertrek		x	x				x	x
Bewaring								x
Opvang						x		

4. Algemene waarborgen voor de bescherming van de persoonlijke levenssfeer

Het wetsvoorstel geeft een aantal algemene waarborgen voor bescherming van de persoonlijke levenssfeer van vreemdelingen.

Wettelijke bescherming en doelbinding

Het wetsvoorstel geeft een heldere juridische grondslag voor het gebruik van biometrische persoonsgegevens in de vreemdelingenketen. Het wetsvoorstel bevat een welbepaalde en uitdrukkelijke omschrijving van de doeleinden van de gegevensverwerking.[6] In de toelichting wordt aangegeven welke afweging is gemaakt tussen enerzijds het belang dat gemoeid is met de verwerking van persoonsgegevens en het belang van de bescherming van die gegevens.
Hiermee is duidelijk voor welke doelen het verzamelen en de raadpleging van de persoonsgegevens is toegestaan. Naast de in het wetsvoorstel opgenomen specifieke waarborgen om de privacy te beschermen gelden ter wettelijke bescherming ook de algemene regels van de Wet bescherming persoonsgegevens (Wbp). Zo gelden bijvoorbeeld de algemene regels van de Wbp over inzage en correctie, het gegevensverkeer naar landen buiten de EU en het toezicht.

Beperkte bewaartermijn

Voor het bepalen van de bewaartermijn van tien jaar is uitsluitend rekening gehouden met de gestelde doelen van de wet. De persoonsgegevens worden niet langer bewaard dan nodig is om deze doelen te bereiken. De mogelijkheden tot function creep, hacken en onbevoegde inzage van de gegevens bestaat na het verlopen van de bewaartermijn niet meer mits deze gegevens adequaat en duurzaam worden vernietigd, zie hierover de beschrijving hieronder over “vernietiging van biometrische gegevens”. [7]

Onafhankelijk toezicht

Het College Bescherming Persoonsgegevens houdt toezicht op de naleving van de Wet bescherming persoonsgegevens en de functionaris voor de gegevensbescherming van het ministerie van Veiligheid en Justitie zal ook toezicht houden op de voorgestelde gegevensverwerking.

Evaluatiebepaling

In lijn met het regeerakkoord van het kabinet Rutte-II worden maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens voorzien van een evaluatiebepaling[8], waarin staat dat vijf jaar na de inwerkingtreding een verslag zal worden uitgebracht over de doeltreffendheid en de effecten van de wet in de praktijk. Bij deze evaluatie wordt de aard en omvang van alle privacyrisico’s doorgelicht om te bezien of er veranderingen in het risicobeeld zijn opgetreden en de risicobeheersende maatregelen adequaat zijn. In dit opzicht is de evaluatiebepaling een risicobeheersende maatregel voor alle geïdentificeerde risico’s.

[6] Zie het tweede lid van het voorgestelde artikel 107 van de Vreemdelingenwet 2000.
[7] Opinion 3/2012 on developments in biometric technologies, Article 29 Data Protection Working Party, retention period, pag. 10.
[8] Bij de bouw van systemen en het aanleggen van databestanden is bescherming van persoonsgegevens uitgangspunt. Daar hoort een zogenaamd privacy impact assessment (PIA) standaard bij. Inbreuken door de overheid zijn voorzien van een horizonbepaling en worden geëvalueerd. Bruggen slaan, regeerakkoord VVD-PvdA, 29 oktober 2012 (pag. 29).

5. Mogelijke privacyrisico’s en risicobeheersende maatregelen

Aan de hand van de volgende vier procesonderdelen zijn de mogelijke privacyrisico’s geïnventariseerd:
- afname van de biometrische persoonsgegevens (vingerafdrukken en de gelaatsopname)
- opslag van de gegevens
- gebruik en wijziging van de gegevens
- verstrekking aan derden
- vernietiging van de gegevens

Per processtap wordt vervolgens aangegeven welke maatregelen getroffen zijn om de kans dat de mogelijke risico’s zich voordoen te minimaliseren.

Afname van biometrische gegevens

Risico’s

1.Kwalitatieve gebreken

Afname van onjuiste biometrische gegevens is feitelijk niet mogelijk.[9] Wel kan het voorkomen dat de afgenomen gelaatsopname niet meer actueel is, bij bijvoorbeeld kinderen of dat de biometrische gegevens worden gekoppeld aan onjuiste persoonsgegevens (zie hierover hetgeen hieronder onder “Fraude” staat vermeld). Er kan sprake zijn van kwalitatieve gebreken van de biometrische informatie indien niet alle vingerafdrukken afgenomen kunnen worden door een tijdelijke of permanente beschadiging aan de vingers (incomplete gegevens)[10]

2. Fraude

Bij het verzamelen van biometrische gegevens bestaat het risico van identiteits- en documentfraude, identiteitsverwisseling en identiteitsdiefstal (mogelijk ook ten nadele van de betrokken vreemdeling) door het koppelen van biometrische gegevens aan de onjuiste persoonsgegevens. Biometrische gegevens kunnen gekoppeld worden aan een verkeerde identiteit; een andere mogelijkheid is dat bij een biometrische mismatch een onjuiste identiteitsvaststelling kan ontstaan. Het blijkt mogelijk om biometrie na te bootsen waardoor fraude met de biometrie zelf mogelijk is.

3. Mismatches

Er bestaat een risico op verkeerde herkenning en kans op mismatch na vergelijking van de afgenomen gegevens met de gegevens uit de BVV. Er kan niet worden aangegeven hoe vaak in de praktijk voorkomt dat de gegevens die worden gebruikt voor verificatie niet matchen met de gegevens uit de BVV. Wel is aangegeven dat dit vooral technische problemen zijn.[11] In het functioneel ontwerp van de BVV is voorzien in de mogelijkheid van ontkoppeling van de gegevens bij een mismatch (de situatie dat biometrische gegevens gekoppeld worden aan een verkeerde naam of verkeerd nummer).

4. Onvoldoende transparantie

De vreemdeling waar de biometrische gegevens van worden verzameld krijgt geen of onvoldoende informatie over de reden van afname, over waar de gegevens voor worden gebruikt en over zijn of haar rechten hierbij. Onvoldoende transparantie bij afname van biometrie (over gegevensgebruik en rechten van de vreemdeling).

[9] Zie hierover Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, adopted 27th April 2012.
[10] Het hangt wel af van de gebruikte techniek, het is met een single finger scanner goed mogelijk om een pink als een middelvinger te registreren, wat het afnemen van een onjuist gegeven is.
[11] De manier waarop de vreemdeling zijn vingers op de scanner legt en de toestand van de huid zijn hierbij van groot belang.

Risicobeheersende maatregelen

1. Kwalitatieve gebreken

Voorgesteld wordt om biometrische persoonsgegevens centraal op te slaan in de BVV zodat deze gegevens door alle ketenpartners kunnen worden gebruikt. Het belang van uniforme kwaliteitseisen en een gestandaardiseerde werkwijze voor het identificeren, registreren, wijzigen en verifiëren van persoonsgegevens in de vreemdelingenketen is hiermee nog groter geworden. In het Protocol Identificatie en Labeling wordt deze werkwijze beschreven[12]. Deze interne werkinstructie voor de ketenpartners zal naar aanleiding van dit wetsvoorstel worden geactualiseerd evenals de Regeling Basisvoorziening vreemdelingen waarin regels zijn gesteld over het beheer van de BVV. Er zijn al instructies en protocollen in gebruik over hoe om te gaan met mutilatie. Het algemeen kader hiervoor zal worden geregeld in de amvb die wordt voorbereid.
Voorts zal er niet uitsluitend worden vertrouwd op de technologie. Een vreemdeling kan niet worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden dat louter wordt genomen op grond van de geautomatiseerde gegevensverwerking. Er zal altijd een menselijke schakel in het identificatieproces betrokken zijn.

2. Fraude

Bij een vermoeden van identiteits- en documentfraude of vermeende identiteitsverwisseling of identiteitsdiefstal worden experts op het gebied van vingerafdrukken (dactyloscopen) ingezet. Dactyloscopen kunnen ook worden ingezet indien een vreemdeling aangeeft dat er sprake is van legaal verblijf terwijl er bij de verificatie van de vingerafdrukken geen match is.
Door de mogelijkheid om standaard codes in het biometrieregister van de BVV op te nemen, kunnen de identificerende en / of verifiërende ketenpartners een aantekening maken over de incomplete gegevens.

Een andere voorziening die van belang is voor de bescherming van de vreemdeling bij identiteitsdiefstal is het centraal meldpunt identiteitsfraude (CMI)[13].

3. Mismatches

Bij het vermoeden van een mismatch worden dactyloscopen ingezet. Door een menselijke beoordeling worden de afgenomen gegevens vergeleken met de gegevens uit de BVV. Door automatische vergelijking wordt ook zoveel mogelijk de kans op een mismatch voorkomen.

4. Transparantie

De ketenpartner die verantwoordelijk is voor de afname van de biometrische gegevens zal bij afname aangeven waar de gegevens voor worden gebruikt (identificatie en verificatie van de vreemdeling). Er vindt geen heimelijke afname of heimelijk gebruik van de persoonsgegevens plaats, zodat de vreemdeling direct bezwaar kan maken of onjuiste of onvolledige gegevens kan laten rectificeren.

[12] Staatscourant 13 juni 2003, nr. 111, pag. 8.

[13] Het CMI is een initiatief van het ministerie van BZK en adviseert en ondersteunt burgers, bedrijven en overheden die te maken hebben met identiteitsfraude of met een fout in de registratie van de persoonsgegevens. Via een online meldingsformulier (beschikbaar via overheid.nl) of het telefoonnummer 1400 kunnen meldingen worden gedaan bij het CMI.

Opslag van biometrische gegevens

Risico's

5. Hacken

Zodra gegevens worden opgeslagen, ontstaat de mogelijkheid dat die gegevens ongewenst worden verspreid. Behalve binnen de organisaties (lekken) is er ook een beveiligingsrisico naar buiten toe. Biometrische gegevens kunnen onbedoeld buiten de organisatie of buiten de BVV terecht komen door onzorgvuldigheid (van een medewerker) of doordat er onrechtmatige toegang tot de opgeslagen biometrische gegevens in de BVV plaatsvindt.

6. Overload aan gegevens

Met dit wetsvoorstel wordt het gebruik van biometrie in de vreemdelingenketen groter. Zo wordt bijvoorbeeld bewerkstelligd dat de biometrische kenmerken die in het kader van de inburgering in het buitenland zijn verwerkt, ook gebruikt kunnen worden in andere contacten met de vreemdelingenketen. De op de diplomatieke of consulaire posten verkregen informatie wordt als gevolg van dit wetsvoorstel rechtstreeks opgeslagen in de BVV. Het wetsvoorstel maakt indirect een grotere opslag van persoonsgegevens mogelijk. Dit kan leiden tot een overload aan gegevens waardoor de beveiliging en de toegankelijkheid van het systeem onder druk kan komen te staan.

7. Afwijkingen in gegevens bij opslag in meederde bestanden

Dit wetsvoorstel wijzigt niet in de bevoegdheid van de ketenpartners om de biometrische gegevens buiten de BVV (de leidende registratie) ook op te slaan in een eigen bestand. Op het moment dat een vreemdeling voor de eerste maal in contact komt met de vreemdelingenketen, wordt door de desbetreffende ketenpartner een gezichtsopname gemaakt en worden er tien vingerafdrukken afgenomen. De ketenpartner verzendt deze biometrische kenmerken digitaal naar de BVV waar vergelijking met eerder afgenomen biometrische kenmerken plaatsvindt. Het wetsvoorstel sluit niet uit dat de ketenpartners in een eigen bestand kopieën van deze persoonsgegevens mogen opslaan. De kans op afwijkingen bij opslag in meerdere bestanden is mogelijk. Zeker als de gegevens in de BVV op een later moment worden aangevuld of gewijzigd (door een andere ketenpartner).

Risicobeheersende maatregelen

5. Hacken

De beveiliging valt binnen de domeinen van de ketenpartners waar nu ook bijzondere persoonsgegevens (gelaatsscans) worden bewaard.
Voor de beveiliging en integriteit van de gegevens in de BVV gelden de beveiligingseisen van de voorziening tot samenwerking Politie Nederland (vtsPN). Indien niet geautoriseerde personen zich onrechtmatig toegang verschaffen tot de BVV of tot de systemen van de ketenpartners dan is dat strafbaar als computervredebreuk. De ketenpartners houden bij hun inkoop- en aanbestedingsprocedure van de eigen beveiligingssystemen ook rekening met de eisen van de vtsPN.

6. Overload aan gegevens

Door het wetsvoorstel is een toename van het aantal registraties in de BVV te verwachten. Dit zal echter niet zo een grote toename van gegevens zijn dat de hoeveelheid niet meer te hanteren is. Technisch is de opslag van de gegevens in de BVV geen probleem, ook de ordening teneinde de gegevens terug te vinden zal geen probleem zijn. Tijdens de bespreking in het Tactisch Regieoverleg is geconcludeerd dat het bij de ketenpartners ook gaat om grote hoeveelheden gegevens, maar niet om een onhanteerbaar grote hoeveelheid gegevens. Bij de bouw van de BVV is reeds rekening gehouden met het verwerken van een dergelijke hoeveelheid gegevens.

7. Afwijking in gegevens bij opslag in meerdere bestanden
Afwijkingen in biometrische gegevens bij opslag in meerdere bestanden kan worden ondervangen door één basisregistratie te benoemen, namelijk de BVV, waarin alle wijzigingen worden doorgevoerd en waaruit blijkt in welke bestanden de desbetreffende gegevens nog meer zijn opgeslagen zodat mogelijke wijzigingen in alle bestanden kunnen worden doorgevoerd.

Gebruik en wijziging van de gegevens

Risico's

8. Function creep
Naarmate er grotere hoeveelheden persoonsgegevens langer en centraal worden opgeslagen en verwerkt, zal een systeem meer privacyrisico's met zich meebrengen.
Het privacyrisico bestaat niet alleen voor bedoeld gebruik, maar ook voor onbedoelde effecten. Zo bestaat het risico dat gegevens voor andere dan de oorspronkelijke doelen zal worden gebruikt (function creep, het fenomeen waarbij - in dit geval- een verzameling van biometrische persoonsgegevens een behoefte zal creëren om ook voor andere dan de oorspronkelijke doelstellingen te worden gebruikt).

9. Onbevoegd gebruik
Als gegevens worden verzameld en opgeslagen, dan is er het risico dat ze in verkeerde handen komen, ook zonder dat er door buitenstaanders in de systemen wordt ingebroken. Zo bestaat het risico dat gegevens door een onbevoegd medewerker van de BVV of van andere ketenorganisaties worden ingezien (ongeautoriseerde toegang).

10. Transparantie over rechten
Het risico bestaat dat er onvoldoende transparantie is over gegevensgebruik en de rechten van de vreemdeling.
De vreemdeling zal bij de afname van de biometrische persoonsgegevens worden verteld waarvoor de gegevens worden afgenomen. Dit is een minimale voorwaarde om gegevens te kunnen rectificeren of bezwaar te maken tegen de afname. In welk bestand en door welke ketenpartners de verzamelde persoonsgegevens vervolgens worden verwerkt kan voor een vreemdeling weinig transparant zijn.

Risicobeheersende maatregelen bij raadpleging, wijziging en gebruik van de gegegevens

8. Function creep
De vreemdeling moet erop kunnen vertrouwen dat de biometrische persoonsgegevens niet anders worden gebruikt dan het doel waarvoor zij mogen worden verwerkt (uitvoering van de Vreemdelingenwet 2000 en de Rijkswet op het Nederlanderschap).
De persoonsgegevens zijn slechts voor een geautoriseerde groep ambtenaren onder bepaalde omstandigheden geautomatiseerd bevraagbaar. In het wetsvoorstel worden de doelen waarvoor de biometrische persoonsgegevens mogen worden geraadpleegd strikt afgebakend. Het beschikbaar stellen van biometrische gegevens voor andere doelen dan genoemd in het (nieuwe) artikel 107 Vreemdelingenwet 2000 is niet toegestaan, ook niet indien dat andere doel verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verkregen. Door het opnemen van een heldere juridische (limitatieve) grondslag in de wet voor het gebruik van de gegevens kan het risico van function creep afdoende worden voorkomen.

9. Onbevoegd gebruik
De getroffen maatregelen om onbevoegd gebruik van de biometrische gegevens te voorkomen zijn de vastgestelde beveiligingseisen, een beperkte opslagtermijn en interne autorisatieregels.

10. Transparantie over rechten
Vreemdelingen kunnen op onverwachte momenten worden geconfronteerd met optreden jegens hen op basis van de verzamelde persoonsgegevens. Onderkend wordt dat vreemdelingen weinig zicht hebben op het gebruik van gegevens, mogelijk zelfs na voorlichting. Informatie voor vreemdelingen die meer willen weten of zijn rechten wenst uit te oefenen is feitelijk wel aanwezig. De algemene bepalingen van de Wet bescherming persoonsgegevens gelden hiervoor. Er wordt een interne werkinstructie tot stand gebracht, zodat alle ketenpartners op gelijke wijze zullen omgaan met de vereiste maatregelen voor het beheer van de gegevens en de rechten van betrokkenen, op grond van de Wet bescherming persoonsgegevens.

Verstrekking aan derden

Het wetsvoorstel geeft in artikel 107, vijfde en zesde lid, van de Vw de volgende limitatieve opsomming van gevallen waarin biometrische gegevens uit de BVV beschikbaar worden gesteld:
- het verstrekken van een reisdocument door een diplomatieke vertegenwoordiging ten behoeve van terugkeer;
- de identificatie van slachtoffers van rampen en ongevallen;
- de opsporing van vervolging van strafbare feiten;
- de toepassing van artikel 55c van het Wetboek van Strafvordering, en
- de uitvoering van de Wet op de inlichten- en veiligheidsdiensten 2002.

Bij de verstrekking ten behoeve van opsporing en vervolging geldt dat vingerafdrukken uit de vreemdelingenadministratie uitsluitend mogen worden verstrekt aan de officier van justitie in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten indien er een redelijk vermoeden bestaat dat de verdachte een vreemdeling is, of in het belang van het onderzoek en het opsporingsonderzoek op een dood spoor is beland, dan wel snel resultaat geboden is bij de opheldering van het misdrijf.

Risico's

11. Er bestaat een risico op onbevoegd gebruik van biometrische gegevens uit de BVV door derden.
Onbevoegd gebruik van biometrische gegevens uit de BVV kan ontstaan door onbevoegde derden die de gegevens uit de BVV gebruiken (zie hierover hetgeen hiervoor over hacken is vermeld) of door bevoegde ketenpartners die de gegevens gebruiken voor andere dan de wettelijk toegestane doelen.

12. Er bestaat een risico op onbevoegd gebruik door diplomatieke vertegenwoordigingen

Risicobeheersende maatregelen om onbevoegde verstrekking aan derden te voorkomen

11. onbevoegd gebruik door derden
Met uitzondering van de diplomatieke vertegenwoordigingen vindt er aan derden geen verstrekking van biometrische gegevens plaats, maar gaat het om een vergelijking van de biometrische gegevens in de vreemdelingenadministratie met gegevens die bij derden aanwezig zijn. Afgezien van het openbaar ministerie heeft geen andere derde partij zich eerder gemeld met een verzoek om informatie uit de BVV. Mocht dit wel gebeuren dan vindt vergelijking alleen plaats onder verantwoordelijkheid van een specifiek daartoe geautoriseerde ambtenaar. Dit zal worden geregeld in de amvb die wordt voorbereid.

12. onbevoegd gebruik door diplomatieke vertegenwoordigingen
De Dienst Terugkeer en Vertrek (DT&V) en de IND beschikken over (interne) instructies in de vorm van procesprotocollen waaronder het proces ter verkrijging van (vervangende) reisdocumenten. De door de IND verstrekte gegevens zijn per definitie vertrouwelijk van aard, zeker waar het asielzoekers betreft. Ook de DT&V verstrekt geen informatie over de inhoud van een mogelijke asielprocedure.

Vernietiging van biometrische gegevens

De biometrische gegevens zullen, op grond van het voorgestelde artikel 107, negende lid, onder b, van de Vw, in ieder geval na beëindiging van het rechtmatig verblijf moeten worden verwijderd uit de vreemdelingenadministratie.

Risico's

11. *Niet tijdige vernietiging*

Er is een risico dat de gegevens na afloop van de wettelijke bewaartermijn niet worden vernietigd.

12. *Geen adequate vernietiging*

Wanneer een digitaal gegeven vernietigd wordt, blijven er altijd restanten van het gegeven achter, waarbij het gegeven onder bepaalde omstandigheden weer te reconstrueren is (met speciale software).

Risicobeheersende maatregelen

11. *Niet tijdige vernietiging*

Vernietigen in de zin van dit wetsvoorstel betekent het zodanig elektronisch vernietigen van gegevens dat deze niet meer door een gebruiker en/of beheerder van een databestand met reguliere autorisatie zichtbaar kunnen worden gemaakt.
In het Tactisch Regieoverleg werd gesignaleerd dat de wijze van vernietiging van deze persoonsgegevens bij de actualisatie van de interne werkinstructie over identificatie en labeling aan de orde dient te komen. In de instructie Basisvoorziening vreemdelingen zijn afspraken tussen de ketenpartners vastgelegd over het beheer van de BVV.
Vooralsnog geldt voor de Basisvoorziening Vreemdelingen dat wanneer de persoon niet meer actief is bij een ketenpartner de gegevens in aanmerking komen voor vernietiging. Er wordt één tot twee keer per jaar een overzicht gemaakt met deze gegevens, die worden aan de ketenpartners aangeboden voor akkoord. De voorziening tot samenwerking Politie Nederland zorgt voor de verwijdering uit de Basisvoorziening Vreemdelingen.

12. *Geen adequate vernietiging*

Het feit dat persoonsgegevens verwijderd en niet meer zichtbaar zijn in de BVV houdt niet in dat de persoonsgegevens ook niet meer te herleiden zijn. Er kunnen digitale sporen achterblijven waarmee de persoonsgegevens mogelijk te reconstrueren zijn. Niet-traceerbare vernietiging van gegevens die ooit in een automatisch gegevensbestand zijn opgenomen blijkt een groot privacy risico. Er zijn nauwelijks risicobeheersende maatregelen te treffen om adequate vernietiging te vergemakkelijken. Vooral door toezicht van de functionaris gegevensbescherming en het Cbp als privacytoezichthouder zou er gecontroleerd moeten worden op adequate vernietiging van de persoonsgegevens.

Privacyrisico's en de risicobeheersende maatregelen die in het kader van dit wetsvoorstel zijn / worden getroffen.

Risico/ Maatregel	1 Afname van onjuiste gegevens	2 Fraude	3 Mismatches	4 Onvoldoende transparantie	5 Hacken	6 Overload	7 Afwijkingen bij opslag in meerdere bestanden	8 Function creep	9 Onbevoegd gebruik	10 Transparantie over rechten	11 Niet tijdige vernietiging	12 Geen adequate vernietiging
Beveiligingseisen vtsPN					x				X			
Menselijke beoordeling/ dactyloscoop	X		X									
Standaard codes in het biometrieregister	X			x								
Beperkte opslagtermijn					X			X	X	X		
Heldere juridische grondslag								X		X	X	
Automatische vergelijking (ketenorganisaties)			X						X	X		
Interne autorisatieregels					x				X			
Inzet dactyloscopen		X										
Interne instructies en protocollen over hoe om te gaan met mutilatie	x	x										
Bureau documentfraude		X										
Door standaard codes in de BVV kunnen de identificerende en /of verifiërende ketenpartners aantekeningen maken over onjuiste / incomplete gegevens	X	X	X									
Strafbaarstelling computervredebreuk					X				X			
Wettelijke bescherming (Wet bescherming persoonsgegevens, bepalingen over inzage en rectificatie)				X				X		X		
Voorlichting				X						X		
Actualisatie PIL	X									X		
Onafhankelijk toezicht door Cbp, functionaris gegevensbescherming	X	X	X	X	X	X	X	X	X	X	X	X
Evaluatiebepaling	X	X	X	X	X	X	X	X	X	X	X	
Integriteits- en kwaliteitsaudits in het vreemdelingenvoorschrift	X	X	X	X	X	X	X	X	X	X	X	X