

ECLI	ECLI:NL:RVS:2018:347
Datum uitspraak	31 januari 2018
Inhoudsindicatie	Bij besluit van 28 maart 2014 heeft de staatssecretaris een aanvraag van [de referent] om vreemdeling A een machtiging tot voorlopig verblijf (hierna: mvv) te verlenen, ingewilligd.

Volledige tekst

Bij deze uitspraak is een [persbericht](#) uitgebracht.

201601536/1/V3 en 201601554/1/V3.

Datum uitspraak: 31 januari 2018

AFDELING

BESTUURSRECHTSPRAAK

Verwijzingsuitspraak op de hoger beroepen van:

de staatssecretaris van Justitie en Veiligheid,

appellant,

tegen de hieronder genoemde uitspraken van de rechtbank Den Haag, zittingsplaats Rotterdam, van 3 februari 2016 in de gedingen tussen

naam vreemdeling Awb-nummer

[vreemdeling A] 15/2131

(hierna: vreemdeling A)

[vreemdeling B] en [referent P] 15/1215

(hierna: vreemdeling B en referent P)

en

de staatssecretaris

Procesverloop

In zaak nr. 201601536/1/V3 (vreemdeling A)

Bij besluit van 28 maart 2014 heeft de staatssecretaris een aanvraag van [de referent] om vreemdeling A een machtiging tot voorlopig verblijf (hierna: mvv) te verlenen, ingewilligd.

Bij besluit van 6 januari 2015 heeft de staatssecretaris het daartegen door vreemdeling A gemaakte bezwaar ongegrond verklaard.

Bij uitspraak van 3 februari 2016 heeft de rechtbank het daartegen door vreemdeling A ingestelde beroep gegrond verklaard, dat besluit vernietigd, het door vreemdeling A

gemaakte bezwaar tegen het besluit van 28 maart 2014 gegrond verklaard en dat besluit herroepen, voor zover daarbij aan hem de verplichting is opgelegd mee te werken aan het afnemen van biometrische gegevens, bepaald dat deze uitspraak in de plaats treedt van het vernietigde besluit en de staatssecretaris opgedragen de in de vreemdelingenadministratie opgenomen biometrische gegevens van vreemdeling A binnen zes weken na de dag van verzending van de uitspraak te vernietigen.

Tegen deze uitspraak heeft de staatssecretaris hoger beroep ingesteld.

Vreemdeling A heeft een schriftelijke uiteenzetting gegeven.

De staatssecretaris en vreemdeling A hebben desgevraagd een nader stuk ingediend.

In zaak nr. 201601554/1/V3 (vreemdeling B en referent P)

Bij besluit van 19 maart 2014 heeft de staatssecretaris een aanvraag van referent P om vreemdeling B een mvv te verlenen, afgewezen.

Bij besluit van 4 april 2014 heeft de staatssecretaris het daartegen door vreemdeling B en referent P gemaakte bezwaar gegrond verklaard en de aanvraag alsnog ingewilligd.

De rechtbank heeft het daartegen door vreemdeling B en referent P ingestelde beroep, gericht tegen de aan vreemdeling B opgelegde verplichting mee te werken aan het afnemen van biometrische gegevens, als bezwaar doorgezonden aan de staatssecretaris.

Bij besluit van 23 december 2014 heeft de staatssecretaris het bezwaar ongegrond verklaard.

Bij uitspraak van 3 februari 2016 heeft de rechtbank het daartegen door vreemdeling B en referent P ingestelde beroep gegrond verklaard, dat besluit vernietigd, het door vreemdeling B en referent P gemaakte bezwaar tegen het besluit van 4 april 2014 gegrond verklaard en dat besluit herroepen, voor zover daarbij aan vreemdeling B de verplichting is opgelegd mee te werken aan het afnemen van biometrische gegevens, bepaald dat deze uitspraak in de plaats treedt van het vernietigde besluit en de staatssecretaris opgedragen de in de vreemdelingenadministratie opgenomen biometrische gegevens van vreemdeling B binnen zes weken na de dag van verzending van de uitspraak te vernietigen.

Tegen deze uitspraak heeft de staatssecretaris hoger beroep ingesteld.

Vreemdeling B heeft een schriftelijke uiteenzetting gegeven.

De staatssecretaris en vreemdeling B hebben desgevraagd een nader stuk ingediend.

In beide zaken

De Afdeling heeft de zaken ter zitting behandeld op 18 januari 2017, waar de staatssecretaris, vertegenwoordigd door mr. H.D. Streef en mr. M.M. van Asperen, advocaat te Den Haag, en vreemdeling A, vreemdeling B en referent P, vertegenwoordigd door mr. D. Schaap, advocaat te Rotterdam, zijn verschenen.

Bij brief van 21 december 2017 heeft de Afdeling partijen medegedeeld dat het onderzoek met toepassing van artikel 8:68 van de Algemene wet bestuursrecht is heropend. Daarbij is medegedeeld dat de Afdeling voornemens is het Hof van Justitie (hierna: het Hof) te verzoeken bij wijze van prejudiciële beslissing uitspraak te doen op de in deze zaken voor te leggen vragen. De tekst van deze vragen was in concept bijgevoegd.

Bij brieven van 15 januari 2018 en 18 januari 2018 hebben de staatssecretaris onderscheidenlijk vreemdeling A, vreemdeling B en referent P hierop gereageerd.

INHOUDSOPGAVE

A. Inleiding

B. Overzicht van zaak nr. 201601536/1/V3

Feiten

Besluiten

C. Overzicht van zaak nr. 201601554/1/V3

Feiten

Besluiten

D. Overzicht in beide zaken

Aangevallen uitspraken

Grievan

E. Toepasselijk wettelijk kader

Recht van de Europese Unie

Nationaal recht

F. Het Nederlandse stelsel

Biometrische gegevens onder de Vreemdelingenwet 1965

(hierna: de Vw 1965)

Biometrische gegevens onder de Vreemdelingenwet 2000

(hierna: de Vw 2000)

Aanvraag tot het verlenen van een mvv onder de Vw 2000

G. Beoordeling grievan in de hoofdgedingen

Grief 1

Grief 2

Aanleiding eerste prejudiciële vraag

Eerste prejudiciële vraag

Aanleiding tweede prejudiciële vraag

Tweede prejudiciële vraag

Aanleiding derde prejudiciële vraag

Derde prejudiciële vraag

H. Conclusie

Beslissing

Bijlage (in de Nederlandse taal)

Het recht van de Europese Unie

Bijlage (in de Franse taal)

Le droit de l'Union Européenne

Overwegingen

A. Inleiding

1. In deze verwijzingsuitspraak is de vraag aan de orde of het verplicht verstrekken van persoonsgegevens in de vorm van een digitale gezichtsopname en tien vingerafdrukken (hierna: biometrische gegevens), voor zover dat Turkse onderdanen betreft, en het verwerken van deze gegevens in een vreemdelingenadministratie in strijd is met artikel 7 van Besluit nr. 2/76 en artikel 13 van Besluit nr. 1/80.

Deze vraag is gerezen in het kader van voor Turkse onderdanen ingediende aanvragen tot het verlenen van een mvv. Bij of krachtens de Vw 2000 is elke onderdaan van een derde land, waaronder dus ook Turkse onderdanen, bij een zodanige aanvraag verplicht om mee te werken aan het afnemen van biometrische gegevens. Het afnemen van deze gegevens heeft automatisch tot gevolg dat deze worden verwerkt in een bestand, in de zin van artikel 2, aanhef en onder a en b, van Richtlijn 95/46/EG (hierna: de Privacyrichtlijn; PB 1995, L 281).

Voorts is bij de Turkse onderdanen de vraag aan de orde of het aan derden beschikbaar stellen van deze biometrische gegevens met het oog op rechtshandhaving op strafrechtelijk gebied kan worden opgevat als een beperking in de zin van artikel 7 van Besluit nr. 2/76 en artikel 13 van Besluit nr. 1/80. Indien dat het geval is, is vervolgens de vraag aan de orde of het aan derden beschikbaar stellen van deze gegevens met het oog op rechtshandhaving op strafrechtelijk gebied noodzakelijk is.

B. Overzicht van zaak nr. 201601536/1/V3

Feiten

2. Vreemdeling A is op 1 januari 1966 geboren en heeft de Turkse nationaliteit. Het Uitvoeringsinstituut werknemersverzekeringen heeft bij besluit van 4 januari 2013 aan de referent voor de arbeid van vreemdeling A als internationaal chauffeur een tewerkstellingsvergunning met een geldigheidsduur van 25 september 2012 tot 25 september 2015 verleend. Vreemdeling A heeft op 1 november 2013 een arbeidsovereenkomst met de referent gesloten om met ingang van 1 december 2013 voor de duur van vijf jaar arbeid als internationaal chauffeur te verrichten.

Besluiten

2.1. De referent heeft op 15 november 2013 een aanvraag ingediend om vreemdeling A een mvv voor het verrichten van arbeid in loondienst te verlenen. Bij besluit van 28 maart 2014 heeft de staatssecretaris deze aanvraag ingewilligd. In dat besluit is, voor zover thans van belang, vermeld dat de mvv alleen wordt verleend als vreemdeling A zijn biometrische gegevens laat afnemen. Vreemdeling A heeft meegewerkt aan het afnemen van deze gegevens. Op 25 april 2015 heeft hij bezwaar gemaakt tegen het afnemen en verwerken van zijn biometrische gegevens. Vreemdeling A is met een mvv Nederland binnengekomen en vervolgens in het bezit gesteld van een verblijfsvergunning regulier voor bepaalde tijd.

2.2. Naar aanleiding van hetgeen vreemdeling A in bezwaar heeft aangevoerd, heeft de staatssecretaris zich in het besluit op bezwaar van 6 januari 2015 op hetzelfde standpunt gesteld als in het besluit op bezwaar van 23 december 2014 in zaak nr. 201601554/1/V3. Dat standpunt wordt onder 3.2. weergegeven.

C. Overzicht van zaak nr. 201601554/1/V3

Feiten

3. Vreemdeling B is op [...] geboren en heeft de Turkse nationaliteit. Hij is op [...] te [plaats] in Turkije in het huwelijk getreden met referent P, geboren op [...], die zowel de Nederlandse als de Turkse nationaliteit heeft.

Besluiten

3.1. Referent P heeft op 17 februari 2014 een aanvraag ingediend om vreemdeling B een mvv voor gezinshereniging te verlenen. Bij besluit van 28 maart 2014 heeft de staatssecretaris haar aanvraag afgewezen, omdat zij niet heeft aangetoond te beschikken over voldoende middelen van bestaan. Bij besluit van 4 april 2014 heeft de staatssecretaris het daartegen door de vreemdeling B en referent P gemaakte bezwaar gegrond verklaard en de aanvraag alsnog ingewilligd. Vreemdeling B heeft meegewerkt aan het afnemen van zijn biometrische gegevens. Vreemdeling B is met een mvv Nederland binnengekomen en op 18 april 2014 in het bezit gesteld van een verblijfsvergunning regulier voor bepaalde tijd. Op 2 mei 2014 hebben hij en referent P bezwaar gemaakt tegen het afnemen en verwerken van deze gegevens.

3.2. Naar aanleiding van hetgeen vreemdeling B en referent P in bezwaar hebben aangevoerd, heeft de staatssecretaris zich in het besluit op bezwaar van 23 december 2014, samengevat, op het standpunt gesteld dat het afnemen en verwerken van biometrische gegevens niet in strijd is met artikel 7 van Besluit nr. 2/76 en artikel 13 van Besluit nr. 1/80.

Volgens de staatssecretaris is het afnemen en verwerken van biometrische gegevens geen nieuwe beperking in de zin van deze bepalingen, omdat zowel onder de Vw 1965 als de Vw 2000 steeds het uitgangspunt is geweest dat een vreemdeling medewerking moet verlenen aan het vastleggen van gegevens met het oog op identificatie. Dat de techniek voor het vastleggen van deze gegevens is gewijzigd, maakt niet dat dit uitgangspunt is gewijzigd. Het afnemen en verwerken van biometrische gegevens vormen weliswaar een aantasting van de rechten in artikel 7 en 8 van het EU Handvest, maar deze aantasting is gerechtvaardigd, gelet op het legitieme doel.

Evenmin is volgens de staatssecretaris het afnemen en verwerken van de biometrische gegevens in strijd met artikel 9 van de Overeenkomst waarbij een associatie tot stand wordt gebracht tussen de Europese Economische Gemeenschap en Turkije (PB 1964, 217; hierna: de Associatieovereenkomst). Anders dan bij burgers van de Unie is de verblijfstitel van Turkse onderdanen bij een eerste toelating niet declaratoir, maar constitutief van aard. Voorts is van belang dat paspoorten van burgers van de Unie van biometrische gegevens zijn voorzien, aldus de staatssecretaris.

D. Overzicht in beide zaken

Aangevallen uitspraken

4. De overwegingen van de rechtbank in de uitspraken van 3 februari 2016 zijn in beide zaken identiek.

4.1. De rechtbank heeft overwogen dat het standpunt van de staatssecretaris dat de verplichting mee te werken aan het afnemen en verwerken van biometrische gegevens een voorwaarde is voor het verlenen van een mvv in wezen betekent dat deze verplichting een formele voorwaarde is voor toelating tot Nederland. Deze voorwaarde is nieuw, omdat deze verplichting - als formele voorwaarde voor toelating - niet gold op de voor artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 relevante data.

4.2. De rechtbank heeft vervolgens overwogen dat het doel van het afnemen en verwerken van biometrische gegevens, te weten het voorkomen en bestrijden van identiteits- en documentfraude, een legitiem doel is, maar dat de verplichting om mee te werken aan het afnemen en verwerken van biometrische gegevens geen evenredig middel is om dit legitieme doel te bereiken.

De rechtbank heeft daartoe overwogen dat de staatssecretaris niet aannemelijk heeft gemaakt dat het verwerken van biometrische gegevens in de in artikel 107, eerste lid, van de Vw 2000 bedoelde vreemdelingenadministratie noodzakelijk is. Gesteld noch gebleken is dat Turkse onderdanen gemiddeld meer dan andere onderdanen van derde landen gebruik maken van een vals of vervalst paspoort of gebruik maken van een authentiek nationaal paspoort, dat is afgegeven op basis van valse of vervalste brondocumenten. Aldus bestaat geen grond om op voorhand te twijfelen aan de identiteit van Turkse onderdanen die om toegang en verblijf in Nederland verzoeken. Dat volgens de staatssecretaris met alleen het opnemen van biometrische gegevens in het verblijfsdocument niet kan worden uitgesloten dat een Turkse onderdaan aan wie dit document is verstrekt onder een andere identiteit eerder een aanvraag tot het verlenen van een verblijfsvergunning heeft ingediend of later een zodanige aanvraag zal indienen, is onvoldoende om het verwerken van de biometrische gegevens wel noodzakelijk te achten. In dit opzicht verschilt deze Turkse onderdaan immers niet van een burger van de Unie die onder een andere identiteit eerder in Nederland heeft verbleven of wellicht zal verblijven en wiens biometrische gegevens niet worden afgenomen en verwerkt in de vreemdelingenadministratie.

Voorts heeft de rechtbank overwogen dat het verstrekken van de biometrische gegevens in de in artikel 107, vijfde lid, van de Vw 2000 omschreven gevallen verder gaat dan noodzakelijk is voor het bereiken van het legitieme doel.

Op grond van deze overwegingen heeft de rechtbank geconcludeerd dat de verplichting mee te werken aan het afnemen van biometrische gegevens, en daarmee aan het verwerken van die gegevens overeenkomstig 107 van de Vw 2000, een nieuwe beperking vormt van de uitoefening van het vrije verkeer van Turkse werknemers, die op grond van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 buiten toepassing moet worden gelaten.

Grievan

5. De grieven van de staatssecretaris in de tegen deze uitspraken ingestelde hoger beroepen zijn in beide zaken identiek.

5.1. Grief 1 is gericht tegen de overweging, die hiervoor onder 4.1. is weergegeven.

De staatssecretaris klaagt in deze grief, zoals nader toegelicht bij het nader stuk en ter zitting bij de Afdeling, dat de rechtbank, door aldus te overwegen, niet heeft onderkend dat een vreemdeling ook onder de

Vw 1965 verplicht was om mee te werken aan de vaststelling, registratie en verificatie van

zijn identiteit. In deze verplichting ligt besloten dat deze vreemdeling geen verblijfsvergunning werd verleend indien zijn identiteit niet kon worden vastgesteld, geregistreerd en geverifieerd. Dat thans biometrische gegevens digitaal kunnen worden afgenomen en verwerkt, behelst geen wijziging van deze verplichting en hetgeen in deze verplichting ligt besloten. Aldus is het afnemen en verwerken van biometrische gegevens geen nieuwe beperking in de zin van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80, aldus de staatssecretaris.

5.2. Grief 2 is gericht tegen de overweging, die hiervoor onder 4.2. is weergegeven.

De staatssecretaris klaagt in deze grief, zoals nader toegelicht bij het nader stuk en ter zitting bij de Afdeling, dat de rechtbank, door aldus te overwegen, niet heeft onderkend dat het afnemen en verwerken van biometrische gegevens in een vreemdelingenadministratie noodzakelijk is voor het nastreven van het door de rechtbank legitiem geachte doel.

Met deze vreemdelingenadministratie is het identificeren en verifiëren van een vreemdeling niet afhankelijk van louter het verblijfsdocument, dat alleen de band met de rechtmatige houder van dat document kan aantonen. Met het verwerken van biometrische gegevens in een vreemdelingenadministratie kan het gebruik van valse of vervalste brondocumenten worden ondervangen en mogelijke fraude met het verblijfsdocument worden voorkomen. Voorts kan een beeld van het verblijfsrechtelijke verleden van een vreemdeling worden verkregen en omdat tien vingerafdrukken worden genomen - in tegenstelling tot de twee voor het verblijfsdocument - is het identificeren en verifiëren ook betrouwbaarder, aldus de staatssecretaris. De termijn van vijf jaar voor bewaring van de biometrische gegevens is noodzakelijk en evenredig ten opzichte van het doel van het betrouwbaar vaststellen van de identiteit van een vreemdeling. Voorts vervalt ingevolge artikel 115 van de Vw 2000 de bevoegdheid om biometrische gegevens te verwerken op 1 maart 2021, zodat ook de periode waarin van deze bevoegdheid gebruik kan worden gemaakt, beperkt is. Het beschikbaar stellen van biometrische gegevens voor de opsporing en vervolging van strafbare feiten dient de strafrechtelijke handhaving van de openbare orde en is binnen de in artikel 107, zesde lid, van de Vw 2000 gestelde grenzen evenredig, aldus de staatssecretaris.

E. Toepasselijk wettelijk kader

6. Wegens de omvang van het voor deze zaken relevante recht van de Europese Unie, wordt in deze uitspraak volstaan met een opsomming. Dat recht is - in de Nederlandse en Franse taal - volledig opgenomen in de bijlagen, die deel uitmaken van deze uitspraak.

Recht van de Europese Unie

(1) de Associatieovereenkomst:

artikel 2 lid 1, artikel 6 en artikel 12;

(2) Aanvullend Protocol bij de Associatieovereenkomst (PB 1972, L 293; hierna: het Aanvullend Protocol):

artikel 36;

(3) Besluit nr. 2/76:

artikel 1, artikel 7 en artikel 13;

(4) Besluit nr. 1/80:

artikel 10 lid 1, artikel 13 en artikel 16;

(5) EU Handvest (PB 2007, C 303):

artikel 7, artikel 8, artikel 51 lid 1 en artikel 52 lid 1 en 3;

(6) Privacyrichtlijn:

artikel 1, artikel 2 onder a) tot en met c), artikel 3, artikel 6 lid 1 onder b), c) en e), artikel 7 lid 1 onder e) en artikel 8 lid 1, 2 en 4;

(7) Verordening (EG) nr. 1030/2002 (PB 2002, L 157), zoals gewijzigd bij Verordening (EG) nr. 380/2008 (PB 2008, L 115; hierna: Verordening (EG) nr. 1030/2002):

punten 5 en 6 van de considerans en artikel 1 lid 1 en 2 onder a), artikel 2 lid 1 onder a), d) en e), artikel 3, artikel 4, artikel 4 bis en artikel 4 ter;

(8) Verordening (EG) nr. 1987/2006 (PB 2006, L 381; hierna: SIS II):

punten 10 tot en 12 van de considerans en artikel 1 lid 2, artikel 2 lid 1, artikel 20 lid 1 en 2 onder e) en f), artikel 21, artikel 24 lid 1 tot en met 3 en artikel 29;

(9) Verordening (EG) nr. 767/2008 (PB 2008, L 218), laatstelijk gewijzigd bij Verordening (EU) nr. 610/2013 (PB 2013, L 182; hierna: de

VIS-verordening):

de punten 5, 10 en 14 van de considerans en artikel 2 onder c) en e) tot en met g), artikel 5 lid 1 onder b) en c), artikel 23, artikel 24 en artikel 25 lid 1 en 2;

(10) Besluit 2008/633/JBZ (PB 2008, L 218; hierna: het VIS-Besluit):

punt 5 van de considerans en artikel 2 lid 1 onder c) en d) en artikel 5 lid 1 onder a) tot en met c);

(11) Verordening (EG) nr. 810/2009 (PB 2009, L 243), laatstelijk gewijzigd bij Verordening (EU) nr. 2016/399 (PB 2016, L 77; hierna: de Visumcode):

artikel 10 lid 1 en 3 onder c) en d) en artikel 13 lid 1 tot en met 3 en lid 7 onder a) en b);

(12) Verordening (EU) nr. 603/2013 (PB 2013, L 180; hierna: de

Eurodac-verordening):

de punten 4 tot en met 6, 8, 10, 15 en 22 van de considerans en artikel 2 lid 1 onder a), i), j) en k), artikel 9 lid 1, artikel 11 lid 1 onder a), artikel 12, artikel 13 lid 1, artikel 14 lid 1, artikel 16 lid 1 en 2 onder a) tot en met c) en artikel 20 lid 1.

Nationaal recht

Vw 2000, Hoofdstuk 1, Inleidende bepalingen, Hoofdstuk 8, Algemene en strafbepalingen en Hoofdstuk 9, Overgangs- en slotbepalingen

Artikel 1 luidt als volgt:

"In deze wet en de daarop rustende bepalingen wordt verstaan onder:

[...];

Europese verordeningen die betrekking hebben op biometrische gegevens:

1 Verordening (EU) nr. 603/2013 (PbEU L 180);

2 Verordening (EU) nr. 767/2008 (PbEU L 218);

3 Verordening (EU) nr. 810/2009 (PbEU L 243);

4 Verordening (EU) nr. 1030/2002 (PbEU L 157);

[...];

gemeenschapsonderdanen:

1°. onderdanen van de lidstaten van de Europese Unie die op grond van het Verdrag betreffende de werking van de Europese Unie gerechtigd zijn een andere lidstaat binnen te komen en er te verblijven;

2°. familieleden van de onder 1° genoemden die de nationaliteit van een derde staat bezitten en die uit hoofde van een ter toepassing van het Verdrag betreffende de werking van de Europese Unie genomen besluit gerechtigd zijn een lidstaat binnen te komen en er te verblijven;

3°. onderdanen van een staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte van 2 mei 1992, die ter zake van binnenkomst en verblijf in een lidstaat rechten genieten die gelijk zijn aan die van burgers van de lidstaten van de Europese Unie;

4°. familieleden van de onder 3° genoemden die de nationaliteit van een derde staat bezitten en die krachtens bovengenoemde Overeenkomst gerechtigd zijn een lidstaat binnen te komen en er te verblijven;

5°. onderdanen van de Zwitserse Bondsstaat, indien zij verblijven op grond van de op 21 juni 1999 te Luxemburg tot stand gekomen Overeenkomst tussen de Europese Gemeenschap en haar lidstaten, enerzijds, en de Zwitserse Bondsstaat, anderzijds, over het vrije verkeer van personen (Trb. 2000, 16 en 86);

6°. familieleden van de onder 5° genoemden die de nationaliteit van een derde staat bezitten en die krachtens de onder 5° genoemde Overeenkomst gerechtigd zijn een lidstaat binnen te komen en er te verblijven;

[...];

persoonsgegevens en verwerking van persoonsgegevens: hetgeen daaronder wordt verstaan in artikel 1 van de Wet bescherming persoonsgegevens;

[...];

vreemdelingen: ieder die de Nederlandse nationaliteit niet bezit en niet op grond van een wettelijke bepaling als Nederlander moet worden behandeld."

Artikel 106a luidt als volgt:

"1. Voor zover op grond van de Europese verordeningen die betrekking hebben op biometrische gegevens, bedoeld in artikel 1, geen gezichtsopname of vingerafdrukken kunnen worden afgenomen en verwerkt, kunnen van een vreemdeling een gezichtsopname en tien vingerafdrukken worden afgenomen en verwerkt voor het vaststellen van de identiteit met het oog op de uitvoering van deze wet. De gezichtsopname en vingerafdrukken worden

vergeleken met de gezichtsopnames en vingerafdrukken in de vreemdelingenadministratie.
[...].

4. Het eerste lid is niet van toepassing op:

- a. gemeenschapsonderdanen, en
- b. de vreemdeling die behoort tot een bij algemene maatregel aangewezen categorie.

[...]."

Artikel 107 luidt als volgt:

"1. Er is een vreemdelingenadministratie, die wordt beheerd door Onze Minister. De vreemdelingenadministratie bevat:

- a. de gezichtsopnames en vingerafdrukken, bedoeld in artikel 106a, eerste lid;
- b. andere persoons- en verwijzingsgegevens van vreemdelingen die volgens een door Onze Minister vastgestelde werkwijze zijn geïdentificeerd en geregistreerd;
- c. andere gegevens, waaronder persoonsgegevens, die van belang zijn voor de uitvoering van deze wet en de Rijkswet op het Nederlanderschap.

2. De vreemdelingenadministratie heeft tot doel de verwerking van:

- a. de in het eerste lid, onder a, bedoelde gegevens voor de uitvoering van deze wet, de Rijkswet op het Nederlanderschap en de daarop gebaseerde regelgeving;

[...].

5. Onverminderd het in het tweede lid, onder a, genoemde doel, en in aanvulling op het bepaalde bij of krachtens artikel 107a, kunnen gegevens als bedoeld in het eerste lid, onder a, uitsluitend beschikbaar worden gesteld met het oog op:

- a. het verstrekken van een reisdocument door een diplomatieke vertegenwoordiging ten behoeve van terugkeer;
- b. de identificatie van slachtoffers van rampen en ongevallen;
- c. de opsporing en vervolging van strafbare feiten;
- d. de toepassing van artikel 55c van het Wetboek van Strafvordering, en
- e. de uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

6. De verstrekking van gegevens betreffende de vingerafdrukken van de vreemdeling uit de vreemdelingenadministratie in de gevallen bedoeld in het vijfde lid, onderdeel c, ten behoeve van de opsporing en vervolging van strafbare feiten vindt slechts plaats in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten en na schriftelijke machtiging van de rechter-commissaris op vordering van de officier van justitie:

- a. indien er een redelijk vermoeden bestaat dat de verdachte een vreemdeling is, of
- b. 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.

[...].

9. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld omtrent:

a. [...];

b. de vernietiging van de in de vreemdelingenadministratie opgenomen gegevens, waarbij geldt dat gezichtsopnames en vingerafdrukken nooit langer worden bewaard dan tien jaar nadat de aanvraag tot het verlenen van een machtiging tot voorlopig verblijf is afgewezen, of, in geval van rechtmatig verblijf, de betrokken vreemdeling wiens rechtmatig verblijf is geëindigd, Nederland aantoonbaar heeft verlaten, dan wel, indien tegen de vreemdeling een inreisverbod is uitgevaardigd of de vreemdeling ongewenst is verklaard, tien jaar na afloop van de geldigheidsduur van het inreisverbod onderscheidenlijk de ongewenstverklaring, en deze gegevens in ieder geval worden vernietigd zodra Onze Minister bekend is dat de betrokkene niet langer behoort tot de categorie vreemdelingen waarvan deze kunnen worden afgenomen;

[...]."

Artikel 115 luidt als volgt:

"1. De bevoegdheid van Onze Minister om op grond van artikel 106a een gezichtsopname en vingerafdrukken van een vreemdeling af te nemen en te verwerken, vervalt zeven jaar na de inwerkingtreding van de wet van

11 december 2013 tot wijziging van de Vreemdelingenwet 2000 in verband met de uitbreiding van biometrische kenmerken in de vreemdelingenketen in verband met het verbeteren van de identiteitsvaststelling van de vreemdeling (Stb. 2014, 2).

2. De in de vreemdelingenadministratie opgenomen gegevens, bedoeld in artikel 107, eerste lid, onderdeel a, worden zeven jaar na de inwerkingtreding van de in het eerste lid bedoelde wet van 11 december 2013 vernietigd.

[...]."

Vreemdelingenbesluit 2000 (hierna: het Vb 2000), Hoofdstuk 8, Algemene en strafbepalingen; Afdeling 3, biometrische gegevens

Artikel 8.27 luidt als volgt:

"De bevoegdheid om vingerafdrukken af te nemen en te verwerken als bedoeld in artikel 106a, eerste en tweede lid, van de Wet, geldt niet ten aanzien van:

a. vreemdelingen die nog niet de leeftijd van zes jaar hebben bereikt, en

b. vreemdelingen bij wie het afnemen van alle vingerafdrukken blijvend fysiek onmogelijk is."

Artikel 8.34 luidt als volgt:

"1. De ambtenaren die het beheer voeren over de vreemdelingenadministratie, hebben rechtstreekse toegang tot de gezichtsopnames en vingerafdrukken in de vreemdelingenadministratie, voor zover zij die toegang nodig hebben voor een goede vervulling van hun taak en Onze Minister hen daartoe heeft gemachtigd. [...]."

Artikel 8.35 luidt als volgt:

"De in de vreemdelingenadministratie opgenomen gezichtsopnames en vingerafdrukken worden niet langer bewaard dan:

- a. vijf jaar nadat de aanvraag tot het verlenen van een machtiging tot voorlopig verblijf is afgewezen;
- b. in geval van rechtmatig verblijf: vijf jaar nadat de betrokken vreemdeling, wiens rechtmatig verblijf is geëindigd, Nederland aantoonbaar heeft verlaten; of
- c. indien tegen de vreemdeling een inreisverbod is uitgevaardigd of de vreemdeling ongewenst is verklaard: vijf jaar na afloop van de geldigheidsduur van het inreisverbod onderscheidenlijk de ongewenstverklaring."

Voorschrift Vreemdelingen 2000 (hierna: het VV 2000), Hoofdstuk 7, Algemene en slotbepalingen

Artikel 7.1I luidt als volgt:

"[...].

3. Ten behoeve van de verstrekking van gegevens uit de vreemdelingenadministratie, bedoeld in artikel 107 van de Wet, op basis van vergelijking van vingerafdruksporen met vingerafdrukken uit het biometrieregister in de vreemdelingenadministratie, zijn slechts de ambtenaren van politie bevoegd die uit hoofde van hun functie als dactyloscopisch expert werkzaam of aangesteld zijn."

F. Het Nederlands stelsel

Biometrische gegevens onder de Vw 1965

7. De Vw 1965 (Stb. 1965, 40) is op 1 januari 1967 in werking getreden (Stb. 1966, 481). Op diezelfde datum is het krachtens die wet vastgestelde Vreemdelingenbesluit 1966 in werking getreden (hierna: het Vb 1966; Stb. 1966, 387).

Een vreemdeling was ingevolge artikel 17, eerste lid, aanhef en onder d, van de Vw 1965 verplicht mee te werken aan het vastleggen van gegevens met het oog op identificatie. Deze bepaling is nader ingevuld bij artikel 65, aanhef en onder b, van het Vb 1966. Op grond van deze bepaling konden biometrische gegevens worden afgenomen, indien daartoe naar het oordeel van de ambtenaar, belast met de grensbewaking of het toezicht op vreemdelingen, gegronde reden bestond. In deel D, Hoofdstuk VII, van de Vreemdelingencirculaire 1966 (hierna: de Vc 1966) was limitatief vermeld in welke gevallen een vreemdeling verplicht was om mee te werken aan het afnemen van biometrische gegevens.

Voormeld artikel 17, eerste lid, aanhef en onder d, bood ook de grondslag voor het voeren van een vreemdelingenadministratie. Uit deel D, Hoofdstuk VII en deel H, onder 2, van de Vc 1966 volgt dat deze administratie uit twee registers bestond: een register voor vreemdelingen met legaal verblijf en een register voor vreemdelingen met illegaal verblijf. De van een vreemdeling afgenomen biometrische gegevens werden gescheiden bewaard: de gezichtsoptname in beide registers en de vingerafdrukken bij het Bureau Centrale Dactyloscopische Dienst.

Biometrische gegevens onder de Vw 2000

7.1. inleiding

De Vw 2000 (Stb. 2000, 495) is op 1 april 2001 in werking getreden (Stb. 2001, 144). Bij Wet van 11 december 2013 tot wijziging van de Vw 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 (Stb. 2014, 2; hierna: de Wet van 11 december 2013) zijn artikel 106a en artikel 115 ingevoegd en is artikel 107 gewijzigd. Ter uitvoering van deze Wet zijn bij Besluit van 21 januari 2014 een aantal bepalingen in het Vb 2000 ingevoegd en gewijzigd. Deze Wet en dit Besluit zijn op 1 maart 2014 in werking getreden (Stb. 2014, 44).

doel van de Wet van 11 december 2013

Het doel van de Wet van 11 december 2013 is het vaststellen, registreren en verifiëren van de identiteit van vreemdelingen en aldus het voorkomen en bestrijden van identiteits- en documentfraude (Kamerstukken II 2011/12, 33 192, nr. 3, blz. 2 en nr. 6, blz. 8). Daartoe bepaalt artikel 106a dat van een vreemdeling biometrische gegevens kunnen worden afgenomen en verwerkt voor de vaststelling van zijn identiteit met het oog op de uitvoering van de Vw 2000.

personele werkingssfeer

Uit artikel 1, gelezen in samenhang met artikel 106a, eerste en vierde lid, van de Vw 2000, volgt dat de bevoegdheid om biometrische gegevens af te nemen, te verwerken en te bewaren in een bestand, voor zover thans van belang, van toepassing is op onderdanen van derde landen, die

(1) langer dan 90 dagen in Nederland willen verblijven voor een verblijfsdoel, anders dan asiel, en daartoe een aanvraag indienen, zoals in deze zaken aanvragen tot het verlenen van een mvv voor arbeid in loondienst onderscheidenlijk gezinshereniging;

(2) illegaal in Nederland verblijven.

Indien de aanvraag tot het verlenen van een mvv of een verblijfsvergunning regulier voor bepaalde tijd wordt ingewilligd, worden de krachtens artikel 106a, eerste lid, van de Vw 2000 afgenomen biometrische gegevens gebruikt voor het document, als bedoeld in artikel 1 van Verordening (EG) nr. 1030/2002 (Kamerstukken II 2011/12, 33 192, nr. 3, blz. 23 en 24). De krachtens artikel 106a, eerste lid, van de Vw 2000 afgenomen biometrische gegevens worden ook automatisch verwerkt in het biometrieregister van de Basisvoorziening Vreemdelingen, dat een onderdeel is van de vreemdelingenadministratie (artikel 107, eerste lid, van de Vw 2000).

De bevoegdheid om biometrische gegevens af te nemen en te verwerken in een bestand is niet van toepassing op:

(1) Nederlanders;

(2) burgers van de Unie, onderdanen van landen, partij bij de Europese Economische Ruimte, en onderdanen van de Zwitserse Bondstaat;

(3) onderdanen van derde landen in het bezit van een visum, bedoeld in artikel 2, onder 2, van de Visumcode;

(4) onderdanen van derde landen die een verzoek om internationale bescherming hebben ingediend, bedoeld in artikel 2, eerste lid, aanhef en onder a, van de Eurodac-verordening;

(5) onderdanen van derde landen die nog niet de leeftijd van zes jaar hebben bereikt en

(6) onderdanen van derde landen bij wie het afnemen van alle vingerafdrukken blijvend fysiek onmogelijk is.

beschikbaar stellen met het oog op rechtshandhaving op strafrechtelijk gebied

De biometrische gegevens kunnen ingevolge artikel 107, vijfde lid, aanhef en onder c, gelezen in samenhang met het zesde lid, van de Vw 2000 aan derden worden verstrekt met het oog op opsporing en vervolging van misdrijven waarvoor voorlopige hechtenis is toegelaten. Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld, dan wel in een aantal, in het Wetboek van Strafrecht en in bijzondere wetten nader omschreven misdrijven, waarop een boete of een gevangenisstraf van ten hoogste één jaar is gesteld. In beide gevallen is vereist dat uit de feiten en omstandigheden blijkt van ernstige bezwaren tegen een verdachte, behoudens bij een verdachte van een terroristisch misdrijf.

Deze gegevens kunnen alleen worden verstrekt in de in artikel 107, zesde lid, van de Vw 2000 omschreven twee gevallen en na schriftelijke machtiging van de rechter-commissaris. Dat is een rechter die belast is met het toezicht op het verloop van een strafrechtelijk opsporingsonderzoek. Deze bepalingen dienen het algemeen belang van de strafrechtelijke handhaving van de rechtsorde en voormeld artikel 107, zesde lid, sluit aan bij de voorwaarden van het VIS-besluit (Kamerstukken II 2011/12, 33 192, nr. 3, blz. 31 en 32).

Uit artikel 8.34 van het Vb 2000, gelezen in samenhang met artikel 7.11, derde lid, van het VV 2000, volgt dat alleen ambtenaren van politie die uit hoofde van hun functie als dactyloscopisch expert werkzaam of aangesteld zijn bevoegd zijn om biometrische gegevens aan derden te verstrekken. Volgens de toelichting bij dit artikel (Stcrt. 2015, 18302) gaat het om ongeveer 45 ambtenaren, die hun werkzaamheden in een voor onbevoegden niet toegankelijke ruimte binnen een beveiligd gebouw uitoefenen.

termijn van bewaren

Ingevolge artikel 107, negende lid, aanhef en onder b, van de Vw 2000 worden de biometrische gegevens nooit langer dan tien jaar bewaard. Naar aanleiding van een door de Eerste Kamer der Staten-Generaal aangenomen motie om de termijn te verkorten naar vijf jaar

(Kamerstukken I 2013/14, 33 192, nr. H) is in artikel 8.35 van het Vb 2000 bepaald dat de biometrische gegevens nooit langer dan vijf jaar worden bewaard. De termijn van vijf jaar is verbonden aan een aantal in deze bepalingen omschreven gevallen. Uit de omschrijving van deze gevallen volgt dat de termijn van bewaring feitelijk langer is dan vijf jaar. Twee in deze bepalingen omschreven gevallen maken dat duidelijk. In het geval van een vreemdeling, wiens verblijfsvergunning regulier voor bepaalde tijd na drie jaar wordt ingetrokken en die twee jaar na deze intrekking Nederland verlaat, bedraagt de daadwerkelijk termijn van bewaring van de biometrische gegevens van deze vreemdeling tien jaar (drie jaar legaal verblijf, twee jaar illegaal verblijf en vijf jaar na vertrek uit Nederland). In het geval dat de staatssecretaris tegen deze vreemdeling ook een inreisverbod met een duur van vijf jaar heeft uitgevaardigd, bedraagt de daadwerkelijk termijn van bewaring vijftien jaar (drie jaar legaal verblijf, twee jaar illegaal verblijf, vijf jaar duur inreisverbod en vijf jaar na het verlopen van de duur van het inreisverbod).

termijn van de Wet van 11 december 2013

De bevoegdheid om biometrische gegevens af te nemen en te verwerken vervalt ingevolge artikel 115, eerste lid, van de Vw 2000 zeven jaar na 1 maart 2014. Uit artikel 115, tweede lid, van de Vw 2000 volgt dat de tussen 1 maart 2014 en 1 maart 2021 afgenomen en verwerkte

biometrische gegevens na 1 maart 2021 moeten worden vernietigd.

Artikel 115 van de Vw 2000 is een zogenoemde horizonbepaling. Deze bepaling heeft tot doel om de Wet van 11 december 2013 na vijf jaar te evalueren en zo nodig wetgeving te initiëren om deze wet niet te laten vervallen. De staatssecretaris heeft in de Eerste Kamer der Staten-Generaal toegezegd om de Wet van 11 december 2013 na drie jaar te evalueren (Handelingen I, 2013/14, item 3, blz. 25). Tijdens de zitting bij de Afdeling is gebleken dat deze evaluatie destijds gaande was, maar ten tijde van de zitting nog niet was afgerond.

Aanvraag tot het verlenen van een mvv onder de Vw 2000

7.2. Een onderdaan van een derde land die langer dan 90 dagen in Nederland wil verblijven voor een regulier verblijfsdoel moet in de regel bij binnenkomst in het bezit zijn van een mvv. Uit artikel 2s van de Vw 2000 volgt dat een mvv door deze onderdaan zelf bij de Nederlandse diplomatieke of consulaire vertegenwoordiging in zijn land van herkomst of door een in Nederland verblijvende referent bij de staatssecretaris kan worden aangevraagd. Ingevolge artikel 54, eerste lid, aanhef en onder c, van de Vw 2000, gelezen in samenhang met artikel 1.31 van het Vb 2000, is deze onderdaan bij de aanvraag verplicht mee te werken aan het afnemen en verwerken van zijn biometrische gegevens. Een mvv kan worden verleend aan een onderdaan van een derde land van wie is aangetoond dat hij voldoet aan de vereisten voor toegang en verlening van een verblijfsvergunning regulier voor bepaalde tijd (artikel 2p van de Vw 2000). Volgens paragraaf B1/3.2.2. van de Vreemdelingencirculaire 2000 (hierna: de Vc 2000) wordt een mvv afgegeven door het plaatsen van een sticker in het geldig document voor grensoverschrijding van een onderdaan van een derde land. Deze sticker bevat de biometrische gegevens van deze onderdaan. Uit artikel 14, tweede lid, van de Vw 2000 volgt dat aan de onderdaan van een derde land aan wie een mvv is verleend en die zich na binnenkomst in Nederland heeft aangemeld, ambtshalve een verblijfsvergunning regulier voor bepaalde tijd wordt verleend. Voordat deze verblijfsvergunning ambtshalve wordt verleend, is de onderdaan van een derde land ingevolge artikel 24, eerste lid, aanhef en onder b, van de Vw 2000, gelezen in samenhang met

artikel 3.102a, van het Vb 2000 verplicht mee te werken aan het afnemen en verwerken van zijn biometrische gegevens.

G. Beoordeling van de grieven in de hoofdgedingen

Grief 1

8. Hetgeen de staatssecretaris in deze grief heeft aangevoerd - dat louter de techniek van afnemen en verwerken van biometrische gegevens is gewijzigd - laat onverlet dat uit artikel 65, aanhef en onder b, van het Vb 1966 (zie pagina 13) volgt dat deze gegevens op de voor artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 relevante data alleen konden worden afgenomen, indien daartoe gegronde reden bestond. Dit voorbehoud is met de op 1 maart 2014 in werking getreden wijziging van artikel 4.45 van het Vb 2000 vervallen. Aldus is de bevoegdheid onder de Vw 2000 om van onderdanen van derde landen, waaronder Turkse onderdanen, biometrische gegevens af te nemen verruimd ten opzichte van deze bevoegdheid onder de Vw 1965. Deze verruiming brengt een wijziging mee in de door de staatssecretaris gestelde voorwaarde voor het verlenen van een mvv, omdat deze voorwaarde thans ook wordt gesteld in een situatie waarin onder de Vw 1965 geen aanleiding bestond om deze voorwaarde te stellen.

8.1. De rechtbank heeft daarom terecht overwogen dat de bevoegdheid om biometrische gegevens af te nemen en te verwerken wat betreft Turkse onderdanen in de in overweging

7.1. omschreven gevallen een nieuwe beperking in de zin van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 is. Grief 1 faalt.

9. Uit de rechtspraak van het Hof (onder meer het arrest van 12 april 2016, Caner Genc, ECLI:EU:C:2016:247, punt 51) volgt dat een beperking in de zin van artikel 13 van Besluit nr. 1/80 is verboden, tenzij deze beperking rechtvaardiging vindt in een dwingende reden van algemeen belang, geschikt is om de verwezenlijking van het nagestreefde legitieme doel te waarborgen en niet verder gaat dan nodig is voor het bereiken daarvan. Grief 2 gaat over de wijze waarop de rechtbank deze toets heeft uitgevoerd.

Grief 2

10. De Afdeling stelt vast dat in hoger beroep niet in geschil is de overweging van de rechtbank dat het afnemen en verwerken van biometrische gegevens rechtvaardiging vindt in een dwingende reden van algemeen belang - het voorkomen en bestrijden van identiteits- en documentfraude - en in beginsel geschikt is om de verwezenlijking van het nagestreefde legitieme doel te waarborgen. In grief 2 klaagt de staatssecretaris dus slechts over de overweging van de rechtbank dat het afnemen en verwerken van biometrische gegevens verder gaat dan nodig is voor het bereiken van het nagestreefde legitieme doel.

Gegeven hetgeen de rechtbank op dit punt heeft overwogen en de staatssecretaris daartegen heeft aangevoerd, is in geschil of (1) het afnemen en verwerken van biometrische gegevens in een vreemdelingenadministratie en (2) de termijn van bewaring in dat bestand verder gaan dan nodig is voor het bereiken van het legitieme doel van het voorkomen en bestrijden van identiteits- en documentfraude. Deze twee punten vormen de aanleiding voor de eerste prejudiciële vraag (overweging 11. tot en met 14.2.). Voorts is in geschil of (3) het aan derden beschikbaar stellen van biometrische gegevens verder gaat dan nodig is voor het bereiken van het legitieme doel van rechtshandhaving op strafrechtelijk gebied. Dit derde punt vormt de aanleiding voor de tweede en derde prejudiciële vraag (overweging 15. tot en met 15.3. onderscheidenlijk 16. tot en met 18.2.).

Aanleiding eerste prejudiciële vraag

11. Hetgeen de staatssecretaris in beroep en hoger beroep over de noodzaak van het verwerken van biometrische gegevens in een bestand heeft aangevoerd, komt er in wezen op neer dat Verordening (EG) nr. 1030/2002 alleen identiteits- en documentfraude door een ander dan de rechtmatige houder van het in deze Verordening bedoelde verblijfsdocument kan voorkomen en bestrijden. Doordat het verblijfsdocument de biometrische gegevens van de rechtmatige houder bevat kan niemand anders dan hij in het maatschappelijk verkeer van dat document gebruik maken.

De nationale regeling voor het verwerken van biometrische gegevens is bedoeld om ook andere vormen van identiteits- en documentfraude te voorkomen en te bestrijden:

(1) identiteits- en documentfraude door een ander dan de rechtmatige houder in het geval dat de beveiliging van de opslag van de biometrische gegevens op het verblijfsdocument wordt omzeild en

(2) identiteits- en documentfraude door de aanvrager (de aanstaande rechtmatige houder) van het verblijfsdocument.

In deze twee gevallen heeft het verwerken van biometrische gegevens in een bestand meerwaarde. Dat bestand maakt het in deze beide gevallen namelijk mogelijk te onderzoeken of (1) de ander die zich voordoeft als de rechtmatige houder van het verblijfsdocument onder

een andere identiteit eerder legaal of illegaal in Nederland heeft verbleven en (2) de aanvrager die een bepaalde identiteit gesteld onder een andere identiteit eerder legaal of illegaal in Nederland heeft verbleven.

Deze twee vormen van identiteits- en documentfraude kunnen dus niet op basis van Verordening (EG) nr. 1030/2002, maar wel met het verwerken van biometrische gegevens in een bestand, worden voorkomen en bestreden. De termijn waarop de biometrische gegevens in het bestand worden bewaard is hierop afgestemd en is ook bedoeld om het plegen van identiteits- en documentfraude te ontmoedigen, aldus de staatssecretaris.

12. Bij de beoordeling van de noodzaak van het verwerken van biometrische gegevens in een bestand in het kader van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 stelt de Afdeling voorop dat biometrische gegevens vallen onder de definitie van persoonsgegevens in de zin van artikel 2, aanhef en onder a, van de Privacyrichtlijn, omdat het "informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon" betreft. Het afnemen en het bewaren van biometrische gegevens vormen een „verwerking van persoonsgegevens" in de zin van artikel 2, aanhef en onder b, van deze richtlijn (zie onder meer het arrest van het Hof van 16 december 2008, Huber, EU:C:2008:724, punt 43).

Hoewel uit de bewoordingen van artikel 8 van de Privacyrichtlijn niet kan worden afgeleid of biometrische gegevens behoren tot de in deze bepaling bedoelde bijzondere categorieën gegevens, neemt de Afdeling dit wel aan. De Hoge Raad heeft op 23 maart 2010 in een strafzaak een arrest gewezen (ECLI:NL:HR:2010: BK6331). In dat arrest heeft de Hoge Raad onder meer op grond van het bepaalde in artikel 16 van de Wet bescherming persoonsgegevens - welke bepaling een omzetting vormt van artikel 8 van de Privacyrichtlijn - overwogen dat een foto een gegeven is waaruit het ras van een persoon kan worden afgeleid en aldus een bijzonder persoonsgegeven is. De Afdeling acht deze overweging ook van toepassing op een foto, die digitaal is opgeslagen en kan worden uitgelezen. Voorts wordt de Privacyrichtlijn met ingang van 25 mei 2018 ingetrokken en vervangen door de op 24 mei 2016 in werking getreden Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (algemene verordening gegevensbescherming; PB 2016 L 119). Uit de bewoordingen van artikel 9, eerste lid, van deze Verordening volgt dat biometrische gegevens een bijzondere categorie gegevens vormen. Deze bepaling biedt daarom een aanknopingspunt om te veronderstellen dat biometrische gegevens ook onder artikel 8, eerste lid, van de Privacyrichtlijn een bijzondere categorie gegevens vormen.

Uit de rechtspraak van het Hof (onder meer het arrest van 21 december 2016, Tele2 Sverige AB en Tom Watson e.a., ECLI:EU:C:2016:970, punt 96) volgt dat uitzonderingen op en beperkingen van de bescherming van de bijzondere categorie persoonsgegevens binnen de grenzen van het strikt noodzakelijke moeten blijven. Binnen deze context moet worden onderzocht of het afnemen en bewaren van biometrische gegevens niet verder gaat dan nodig is voor het verwezenlijken van het legitieme doel van het voorkomen en bestrijden van identiteits- en documentfraude (vergelijk de punten 46 en 47 van het arrest van het Hof van 17 oktober 2013, Schwarz, ECLI:EU:C:2013:670).

Uit paragraaf B1/3.1. van de Vc 2000 volgt dat de Nederlandse ambassade de biometrische gegevens van een Turkse onderdaan die een aanvraag tot het verlenen van een mvv heeft ingediend in Turkije afneemt. De verdere verwerking van deze gegevens vindt in Nederland plaats.

Omdat het afnemen en verwerken niet goed los van elkaar zijn te zien, zal de Afdeling in deze zaken het antwoord op de vraag of de nieuwe beperking - het afnemen en verwerken

van biometrische gegevens van - voor zover het Turkse onderdanen betreft- niet verder gaat dan nodig is voor het bereiken van het legitieme doel van het voorkomen en bestrijden van identiteits- en documentfraude onderzoeken aan de hand van het vereiste van "strikte noodzaak" in het kader van de Privacyrichtlijn.

13. Dat antwoord is naar het oordeel van de Afdeling niet onmiddellijk en eenduidig te geven.

Eenzijds kan worden betoogd dat het afnemen en verwerken van biometrische gegevens in een bestand de doeltreffendheid van het voorkomen en bestrijden van identiteits- en documentfraude vergroot, omdat - zoals de staatssecretaris in wezen heeft betoogd (zie hiervoor overweging 11) - met een bestand ook andere vormen van deze fraude kunnen worden voorkomen en bestreden.

De biometrische gegevens op het verblijfsdocument tonen alleen het verband tussen dat document en de rechtmatige houder aan. Deze biometrische gegevens tonen niet de door deze houder gestelde identiteit aan. Dat laatste kan wel met een bestand worden onderzocht. Een bestand maakt het immers mogelijk te onderzoeken of de biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, overeenkomen met eerder afgenomen en in dat bestand opgeslagen biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen. Indien de biometrische gegevens overeenkomen met eerder afgenomen en in het bestand opgeslagen biometrische gegevens kan worden onderzocht of bij deze twee identieke biometrische gegevens dezelfde of een andere identiteit is gesteld. Indien de eerder gestelde identiteit verschilt van de thans door de aanstaande rechtmatige houder gestelde identiteit, is de door deze onderdaan gepleegde identiteitsfraude aangetoond. Als deze onderdaan daarbij een authentiek nationaal paspoort heeft overgelegd, is niet uitgesloten dat voor het verwerven van dit authentiek nationaal paspoort gebruik is gemaakt van valse of vervalste brondocumenten. Deze vorm van identiteits- en documentfraude is aan het toenemen, omdat het moeilijker is geworden om identiteits- en reisdocumenten te vervalsen of na te maken, zo kan uit een mededeling van de Commissie aan het Europees Parlement en de Raad van 8 december 2016 (COM(2016) 790) worden afgeleid.

Aangezien biometrische gegevens een belangrijk element vormen om de juiste identiteit van een persoon vast te stellen (vergelijk punt 5 van de considerans van de Eurodac-verordening en de punten 27 en 59 van het arrest Schwarz), vergemakkelijkt een bestand met deze gegevens aldus de betrouwbare identificatie en verificatie van onderdanen van derde landen (vergelijk punt 10 en punt 12 van de considerans van de VIS-verordening onderscheidenlijk SIS II) en daarmee de bestrijding van identiteits- en documentfraude (vergelijk artikel 2, aanhef en onder c, van de VIS-verordening).

Een bestand met biometrische gegevens vergroot dan ook de doeltreffendheid van en dient aldus het voorkomen en bestrijden van identiteits- en documentfraude. Zo beschouwd kan het afnemen en verwerken van deze gegevens in een bestand strikt noodzakelijk zijn.

13.1. Anderzijds kan worden betoogd dat uit de systematiek van artikel 8 van de Privacyrichtlijn volgt dat de hoofdregel is dat geen biometrische gegevens worden verwerkt, waarop volgens het in dit geval toepasselijke vierde lid van deze bepaling een uitzondering kan worden gemaakt om redenen van zwaarwegend algemeen belang. Uit de regeling in de Vw 2000, zoals onder 7.1. beschreven, volgt daarentegen dat de hoofdregel is dat de biometrische gegevens van alle onderdanen van derde landen, waaronder Turkse onderdanen, worden afgenomen en verwerkt, behalve van diegene die nog niet de leeftijd van zes jaar hebben bereikt en bij wie het afnemen van alle vingerafdrukken blijvend fysiek

onmogelijk is. Dat onderdanen van derde landen, waaronder Turkse onderdanen, in het bezit van een visum of die een verzoek om internationale bescherming hebben ingediend zijn uitgezonderd is louter daarin gelegen dat hun biometrische gegevens reeds in het VIS of Eurodac zijn verwerkt en de staatssecretaris ook toegang heeft tot deze bestanden om biometrische gegevens te vergelijken. De hoofdregel onder de nationale regeling voor het verwerken van biometrische gegevens ("toegestaan, behoudens"...) is derhalve tegengesteld aan de hoofdregel van artikel 8 van de Privacyrichtlijn ("niet toegestaan, tenzij...") Voorts volgt uit de regeling in de Vw 2000 dat alleen het indienen van een aanvraag voor een verblijf van langer dan 90 dagen, anders dan asiel, en illegaal verblijf al voldoende is om de biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen af te nemen en te verwerken in een bestand. Deze regeling is dus algemeen van toepassing op iedere onderdaan van een derde land, waaronder een Turkse onderdaan, ook als geen aanknopingspunt bestaat dat zij gebruik maken van een vals of vervalst paspoort of een authentiek nationaal paspoort, dat is afgegeven op basis van valse of vervalste brondocumenten (vergelijk het arrest Tele2 Sverige AB en Tom Watson e.a., punt 105).

14. Bij het onderzoek of wordt voldaan aan het vereiste van strikte noodzaak speelt ook de termijn van bewaring een rol. Volgens artikel 6, eerste lid, aanhef en onder e, van de Privacyrichtlijn, voor zover thans van belang, mogen persoonsgegevens immers niet langer worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt noodzakelijk is.

14.1. Het bewaren van biometrische gegevens in een bestand vergroot de doeltreffendheid van het voorkomen en bestrijden van identiteits- en documentfraude. Het aantal in een bestand opgeslagen biometrische gegevens neemt immers tijdens de termijn van bewaring toe en daarmee ook de kans om identiteits- en documentfraude daadwerkelijk op te sporen en te bestrijden. Aldus is niet uit te sluiten dat de mogelijkheid om biometrische gegevens voor een langere termijn te bewaren het plegen van identiteits- en documentfraude ontmoedigt en vermindert.

Het bewaren van biometrische gegevens in een bestand voor een langere termijn vergroot dan ook de doeltreffendheid van en dient aldus het voorkomen en bestrijden van identiteits- en documentfraude. Daarmee gaat het stellen van een langere termijn niet verder dan strikt noodzakelijk is voor het bereiken van het legitieme doel.

14.2. Het voorgaande laat onverlet dat het antwoord op de vraag welke termijn vervolgens als strikt noodzakelijk kan worden aangemerkt niet onmiddellijk is gegeven.

Uit hetgeen onder 7.1. over de termijn van bewaring van de afgenomen biometrische gegevens onder de Vw 2000 is vermeld, volgt dat - ook al is wettelijk bepaald dat deze gegevens nooit langer dan vijf jaar worden bewaard - de termijn van bewaring feitelijk langer kan zijn, omdat deze termijn onder meer is gekoppeld aan de duur van het verblijf (zowel legaal als illegaal) en daarmee voor iedere onderdaan van een derde land, waaronder een Turkse onderdaan, kan verschillen.

Daarentegen zijn de in onderscheidenlijk artikel 29, tweede lid, van het SIS II, artikel 23, eerste lid, van de VIS-verordening en artikel 12, eerste lid, en artikel 16, eerste lid, van de Eurodac-verordening gestelde termijnen voor het bewaren van biometrische gegevens ook daadwerkelijk de feitelijke termijnen. De termijnen zijn in beginsel voor iedere onderdaan van een derde land op wie deze Verordeningen van toepassing zijn gelijk.

Hoewel de duur van de termijn van bewaring onder de Vw 2000 anders is dan onder de

Verordeningen, sluit dat niet uit dat de in het nationaal recht gekozen duur noodzakelijk is (zie het arrest van het Hof van 18 oktober 2012, X NV, ECLI:EU:C:2012:635, punt 37). Het vergelijken van deze twee stelsels binnen hetzelfde rechtsgebied, waaraan dezelfde doelstelling ten grondslag ligt - het vaststellen van de juiste identiteit om identiteits- en documentfraude te voorkomen en te bestrijden - kan evenwel inzicht bieden voor het beantwoorden van de vraag welke termijn noodzakelijk kan worden geacht.

In dit kader overweegt de Afdeling dat de langste termijn van alle in de Verordeningen gestelde termijnen is gesteld in artikel 12, eerste lid, van de Eurodac-verordening: de vingerafdrukken van asielzoekers worden tien jaar na de datum van het afnemen daarvan bewaard. Uit punt 22 van de considerans kan worden afgeleid dat feitelijk na deze termijn het doel van de bewaring, als omschreven in de punten 4 en 5 van de considerans, is vervallen, zodat bewaring voor dat doel niet meer noodzakelijk is. Voorts wordt gewezen op de termijn van het bewaren van gegevens in de VIS-verordening. Hoewel deze Verordening betrekking heeft op een visum voor kort verblijf (ten hoogste 90 dagen binnen een periode van 180 dagen), is een mvv ook een visum, zij het voor lang verblijf (langer dan 90 dagen; zie overweging 7.2.). In zoverre is deze Verordening dan ook van belang. Uit artikel 23 van de VIS-verordening volgt dat de termijn van bewaren ten hoogste vijf jaar bedraagt. Evenals het geval is bij punt 22 van de Eurodac-verordening, kan uit punt 14 van de considerans van de VIS-verordening worden afgeleid dat feitelijk na deze termijn bewaring om de doelstellingen van het VIS te verwezenlijken niet meer noodzakelijk is.

Hieruit kan worden afgeleid dat de termijn van bewaring, ook al zal niet in alle gevallen het doel van de bewaring worden bereikt, niet onbeperkt mag zijn. Deze relativering blijkt niet bij de termijn van bewaring onder de Vw 2000. Naast de twee voorbeelden in overweging 7.1. op pagina 16 van deze uitspraak, kan een derde voorbeeld dat verduidelijken. In het geval dat een rechtmatig verblijvende Turkse onderdaan besluit om niet de Nederlandse nationaliteit te verwerven, is de termijn van het bewaren van zijn biometrische gegevens gelijk aan de duur van zijn rechtmatig verblijf. Bij een rechtmatig verblijf van bijvoorbeeld vijftien jaar is de termijn van bewaring dan ook vijftien jaar, ook al is bij aanvang van of tijdens deze termijn van geen enkel aanknopingspunt gebleken om te veronderstellen dat deze onderdaan identiteits- en documentfraude heeft gepleegd of gepoogd te plegen.

Eerste prejudiciële vraag

14.3. Omdat voor de beoordeling van grief 2 in zoverre een nadere uitleg van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 nodig is, ziet de Afdeling zich genoodzaakt het Hof de volgende vraag voor te leggen:

1a. Moeten artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 aldus worden uitgelegd dat deze bepalingen zich niet verzetten tegen een nationale regeling die voorziet in het algemeen verwerken en bewaren van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, in een bestand in de zin van artikel 2, aanhef en onder a en b, van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281), omdat deze nationale regeling niet verder gaat dan nodig is voor het verwezenlijken van het met deze regeling nagestreefde legitieme doel om identiteits- en documentfraude te voorkomen en bestrijden?

1b. Is daarbij van belang dat de duur van het bewaren van de biometrische gegevens is gekoppeld aan de duur van het legale en/of illegale verblijf van onderdanen van derde landen,

waaronder Turkse onderdanen?

Aanleiding tweede prejudiciële vraag

15. Uit hetgeen onder 7.1. is vermeld, volgt dat een ander doel van de Wet van 11 december 2013 de strafrechtelijke handhaving van de rechtsorde is. Uit hetgeen de rechtbank heeft overwogen (zie hiervoor onder 4.2. op pagina 7 van deze uitspraak), kan worden afgeleid dat zij het in het kader van dit doel verstrekken van biometrische gegevens aan derden (artikel 107, vijfde lid, van de Vw 2000) ook als een beperking in de zin van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 heeft opgevat.

15.1. De Afdeling staat voor de vraag of de rechtbank terecht tot dat oordeel is gekomen.

Het Hof heeft in onder meer het arrest van 21 oktober 2003, Abatay en Sahin, ECLI:EU:C:2003:572, het begrip "beperking" uitgelegd als alle nieuwe nationale maatregelen die tot doel of tot gevolg hebben dat de gebruikmaking door een Turks staatsburger van het vrij verkeer van werknemers op het nationale grondgebied, strengere voorwaarden worden gesteld dan die welke golden bij de inwerkingtreding van Besluit nr. 1/80.

Die rechtspraak heeft betrekking op nationale maatregelen die rechtstreeks raken aan de rechten van arbeid en verblijf onderscheidenlijk vestiging en dienstverlening.

15.2. De Afdeling is bekend met de rechtspraak van het Hof, waaruit volgt dat de artikelen 34, 45 en 49 van het Verdrag betreffende de werking van de Europese Unie (hierna: het VWEU) niet in de weg staan aan nationale maatregelen, indien de gestelde beperkende werking daarvan te onzeker en indirect is om op grond daarvan te kunnen aannemen dat het vrij verkeer van goederen, het vrij verkeer van werknemers of de vrijheid van vestiging worden belemmerd (zie de arresten van 7 maart 1990, Krantz, ECLI:EU:C:1990:97, punt 11, van 20 juni 1996, Semeraro Casa Uno, ECLI:EU:C:1996:242, punt 32, van 27 januari 2000, Graf, ECLI:EU:C:2000:49, punt 24-25, van 1 april 2008, Regering van de Franse Gemeenschap en Waalse regering, ECLI:EU:C:2008:178, punt 51, en van 7 april 2011, Francesco Guarnieri & Cie, ECLI:EU:C:2011:217, punt 17). Uit onder meer het laatste arrest blijkt dat dit ook het geval kan zijn indien de betrokken nationale maatregel onderscheid maakt naar nationaliteit.

15.3. De door het Hof in deze arresten gekozen benadering zou ook kunnen worden toegepast bij de uitleg van het begrip "beperking" in artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80. Het Hof heeft het begrip "belemmering" in de rechtspraak over de artikelen 34, 45 en 49 van het VWEU zeer ruim uitgelegd, maar voor zover het Hof dat begrip heeft begrensd, zou een dergelijke begrenzing temeer kunnen gelden voor het begrip "beperking". Indien deze rechtspraak van overeenkomstige toepassing is, moet immers worden beoordeeld of het effect van het aan derden beschikbaar stellen van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, op de toegang tot de werkgelegenheid te onzeker en indirect is om te kunnen aannemen dat sprake is van een beperking.

Gelet op deze rechtspraak zou kunnen worden betoogd dat het aan derden beschikbaar stellen van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, ten behoeve van onder meer de opsporing en vervolging van strafbare feiten een toekomstige en hypothetische gebeurtenis is, omdat het afhankelijk is van het door de betrokken onderdaan van een derde land, waaronder een Turkse onderdaan, eventueel plegen van strafbare feiten. Aldus is geen sprake van een beperking.

Tweede prejudiciële vraag

15.4. Het is echter niet zeker of de in overweging 15.2 bedoelde rechtspraak van overeenkomstige toepassing is bij de uitleg van het begrip "beperking" in voormeld artikel 7 onderscheidenlijk voormeld artikel 13. De Afdeling ziet zich daarom genoodzaakt het Hof de volgende vraag voor te leggen:

2. Moet artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 aldus worden uitgelegd dat een nationale regeling geen beperking in de zin van deze bepalingen vormt, indien het effect van de nationale regeling op de toegang tot de werkgelegenheid, als bedoeld in deze bepalingen, te onzeker en indirect is om te kunnen aannemen dat deze toegang wordt belemmerd?

Aanleiding derde prejudiciële vraag

16. Voor het geval moet worden aangenomen dat het aan derden beschikbaar stellen van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, uit een bestand met het oog op de strafrechtelijke handhaving van de rechtsorde een beperking in de zin van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 is, overweegt de Afdeling als volgt.

17. Omdat de in artikel 107, zesde lid, van de Vw 2000 gestelde voorwaarden waaronder biometrische gegevens aan derden beschikbaar kunnen worden gesteld aansluiten bij artikel 5 van het VIS-besluit (zie overweging 7.1. op pagina 15 van deze uitspraak), zal de Afdeling bij de beoordeling aannemen dat het doel van de Wet van 11 december 2013 - de strafrechtelijke handhaving van de rechtsorde - identiek is aan een van de doelstellingen van het VIS, te weten rechtshandhaving (voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten). Deze doelstelling ligt ook ten grondslag aan de Eurodac-verordening en aan het voorstel tot herschikking van deze Verordening (COM(2016) 272 def). Deze doelstelling is ook ten grondslag gelegd aan het voorstel voor een Verordening tot instelling van een inreis-uitreisstelsel (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen van de Europese Unie overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandavingsdoeleinden en tot wijziging van Verordening (EG) nr. 767/2008 en Verordening (EU) nr. 1077/2011 (COM (2016) 194 def).

18. Uit artikel 3, tweede lid, eerste streepje, van de Privacyrichtlijn volgt dat deze richtlijn niet rechtstreeks van toepassing is op het beschikbaar stellen van biometrische gegevens voor rechtshandhaving op strafrechtelijk gebied. De verwerking van persoonsgegevens voor dit doel is wel mogelijk onder Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB 2016 L 119). Deze richtlijn is evenwel op 5 mei 2016, dus na het nemen van de besluiten op bezwaar in deze zaken, in werking getreden. Kaderbesluit 2008/977/JBZ is naar het oordeel van de Afdeling niet van toepassing, omdat het toepassingsgebied van dit kaderbesluit is beperkt tot de verwerking van persoonsgegevens die worden doorgegeven of beschikbaar gesteld tussen lidstaten.

Niettemin is van belang om te bezien of het recht van Unie wellicht anderszins op het

beschikbaar stellen van biometrische gegevens voor rechtshandhaving op strafrechtelijk gebied van toepassing is.

Als het beschikbaar stellen van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, uit een bestand met het oog op de strafrechtelijke handhaving van de rechtsorde een beperking in de zin van artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 is, moet ook in dit kader worden beoordeeld of deze beperking niet verder gaat dan nodig is voor het bereiken van voormeld legitiem doel. Het standpunt van de staatssecretaris dat deze beperking gerechtvaardigd is, duidt erop dat het recht van de Unie ten uitvoer wordt gebracht in de zin van artikel 51, eerste lid, van het EU Handvest (vergelijk het arrest van het Hof van 30 april 2014, *Pfleger*, ECLI:EU:C:2014:281, punten 35 en 36).

Het voor rechtshandhaving op strafrechtelijk gebied beschikbaar stellen van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, valt onder artikel 7 en 8 van het EU Handvest (vergelijk het arrest van het Hof van 8 april 2014, *Digital Rights Ireland*, ECLI:EU:C:2014:238, punt 29).

Zoals het Hof ook heeft overwogen (arrest van 6 oktober 2015, *Schrems*, ECLI:EU:C:2015:650, punt 92) vereist de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven.

18.1. Enerzijds kan worden betoogd dat het beschikbaar stellen van in een vreemdelingenadministratie opgenomen biometrische gegevens de doeltreffendheid van de rechtshandhaving vergroot. Indien het vermoeden bestaat dat een - nog niet aangehouden - verdachte van een misdrijf een vreemdeling is, kan in het geval van een vingerafdruk of vingerafdrukken op de plaats van het misdrijf, snel en volledig informatie worden ingewonnen over diens identiteit en aldus worden bijgedragen aan het onderzoek van het misdrijf (vergelijk overweging 14 van de Eurodac-verordening). Dat is ook het geval bij een aangehouden verdachte waarvan wordt vermoed dat het een vreemdeling is en die niet in het bezit is van een verblijfsdocument - hetzij omdat hij dat document niet bij zich heeft, hetzij omdat hij dat document niet heeft omdat hij illegaal hier te lande verblijft - of gebruik maakt van een verblijfsdocument dat niet van hem is.

Het beschikbaar stellen van biometrische gegevens in deze situaties kan dus waardevol zijn als hulpmiddel voor en dient aldus het bereiken van het legitieme doel van rechtshandhaving. Daarmee zou deze beperking van de in artikel 7 en 8 van het EU Handvest gewaarborgde rechten noodzakelijk kunnen worden geacht in de zin van artikel 52, eerste lid, van dat Handvest.

18.2. Het vorenstaande kan worden betwijfeld bij een aangehouden verdachte waarvan wordt vermoed dat het een vreemdeling is en die het verblijfsdocument bij zich heeft. In dat geval kan de identiteit van de aangehouden verdachte in de regel worden achterhaald aan de hand van de op dat document opgeslagen biometrische gegevens. Indien aan de hand van het vergelijken van de vingerafdrukken is aangetoond dat de aangehouden verdachte de rechtmatige houder is van het verblijfsdocument, bestaat geen aanleiding om in deze situatie de in de vreemdelingenadministratie opgenomen biometrische gegevens ter beschikking te stellen.

Los van het vorenstaande volgt uit hetgeen hiervoor in overweging 7.1. is vermeld dat de in artikel 107, vijfde lid, van de Vw 2000 omschreven categorie misdrijven op grond waarvan de

biometrische gegevens beschikbaar kunnen worden gesteld ruimer is dan de in artikel 5, eerste lid, onder a, van het VIS-Besluit en artikel 20, eerste lid, onder a, van de Eurodac-verordening bedoelde misdrijven. Zo kunnen krachtens artikel 107, vijfde lid, van de Vw 2000 de biometrische gegevens van een vreemdeling beschikbaar worden gesteld bij verdenking van het plegen van een aantal misdrijven, waarop een vrijheidsstraf van ten hoogste één jaar staat. Hoewel onder de Vw 2000 aldus meer dan onder het VIS-besluit en de (voorgestelde) Verordeningen biometrische gegevens ter beschikking kunnen worden gesteld, sluit dat niet uit dat deze nationaalrechtelijke keuze noodzakelijk is (zie arrest X NV, punt 37). Het vergelijken van deze twee stelsels binnen hetzelfde rechtsgebied, waaraan dezelfde doelstelling ten grondslag ligt - rechtshandhaving - kan evenwel inzicht bieden voor het beantwoorden van de vraag in welke gevallen het beschikbaar stellen van biometrische gegevens voor rechtshandhaving noodzakelijk kan worden geacht.

Derde prejudiciële vraag

18.3. In het licht van hetgeen hiervoor is overwogen is voor de Afdeling niet duidelijk of het beschikbaar stellen van biometrische gegevens van Turkse onderdanen, noodzakelijk is in de zin van artikel 52, eerste lid, van het EU-Handvest. Daarom legt de Afdeling het Hof de volgende vraag voor:

3a. Indien het antwoord op vraag 2 is dat een nationale regeling die het mogelijk maakt de biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, uit een bestand aan derden beschikbaar te stellen met het oog op voorkomen, opsporen en onderzoeken van - al dan niet terroristische - misdrijven een nieuwe beperking is, moet artikel 52, eerste lid, gelezen in samenhang met artikel 7 en artikel 8 van het Handvest van de grondrechten van de Europese Unie, dan aldus worden uitgelegd dat het zich verzet tegen een dergelijke nationale regeling?

3b. Is daarbij van belang dat deze onderdaan op het moment dat hij als verdachte van een misdrijf is aangehouden het verblijfsdocument, waarop zijn biometrische gegevens zijn opgeslagen, bij zich heeft?

H. Conclusie

19. De behandeling van het hoger beroep zal worden geschorst totdat het Hof uitspraak heeft gedaan.

Beslissing

De Afdeling bestuursrechtspraak van de Raad van State:

I. verzoekt het Hof van Justitie bij wege van prejudiciële beslissing uitspraak te doen op de volgende vragen:

1a. Moeten artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 aldus worden uitgelegd dat deze bepalingen zich niet verzetten tegen een nationale regeling die voorziet in het algemeen verwerken en bewaren van biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, in een bestand in de zin van artikel 2, aanhef en onder a en b, van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281), omdat deze nationale regeling niet verder gaat dan nodig is voor het verwezenlijken van het met deze regeling nagestreefde legitieme doel om identiteits- en documentfraude te voorkomen en bestrijden?

1b. Is daarbij van belang dat de duur van het bewaren van de biometrische gegevens is gekoppeld aan de duur van het legale en/of illegale verblijf van onderdanen van derde landen, waaronder Turkse onderdanen?

2. Moet artikel 7 van Besluit nr. 2/76 onderscheidenlijk artikel 13 van Besluit nr. 1/80 aldus worden uitgelegd dat een nationale regeling geen beperking in de zin van deze bepalingen vormt, indien het effect van de nationale regeling op de toegang tot de werkgelegenheid, als bedoeld in deze bepalingen, te onzeker en indirect is om te kunnen aannemen dat deze toegang wordt belemmerd?

3a. Indien het antwoord op vraag 2 is dat een nationale regeling die het mogelijk maakt de biometrische gegevens van onderdanen van derde landen, waaronder Turkse onderdanen, uit een bestand aan derden beschikbaar te stellen met het oog op voorkomen, opsporen en onderzoeken van - al dan niet terroristische - misdrijven een nieuwe beperking is, moet artikel 52, eerste lid, gelezen in samenhang met artikel 7 en artikel 8 van het Handvest van de grondrechten van de Europese Unie, dan aldus worden uitgelegd dat het zich verzet tegen een dergelijke nationale regeling?

3b. Is daarbij van belang dat deze onderdaan op het moment dat hij als verdachte van een misdrijf is aangehouden het verblijfsdocument, waarop zijn biometrische gegevens zijn opgeslagen, bij zich heeft?

II. schorst de behandeling van het hoger beroep tot het Hof van Justitie uitspraak heeft gedaan en houdt iedere verdere beslissing aan.

Aldus vastgesteld door mr. N. Verheij, voorzitter, en mr. G.M.H. Hoogvliet en mr. C.M. Wissels, leden, in tegenwoordigheid van mr. J. van de Kolk, griffier.

w.g. Verheij w.g. Van de Kolk

voorzitter griffier

Uitgesproken in het openbaar op 31 januari 2018

347.

Bijlage (in de Nederlandse taal)

Het Recht van de Europese Unie

Associatieovereenkomst

Artikel 2 luidt:

"1. De Overeenkomst heeft ten doel de gestadige en evenwichtige versterking van de commerciële en economische betrekkingen tussen de Partijen te bevorderen, met volledige inachtneming van de noodzaak de versnelde ontwikkeling van de economie van Turkije en de verruiming van de werkgelegenheid en de verbetering der levensomstandigheden van het Turkse volk te verzekeren.

[...]."

Artikel 6 luidt:

"Ten einde de toepassing en de geleidelijke ontwikkeling van de associatieregeling te

verzekeren, verenigen de Overeenkomstsluitende Partijen zich in een Associatieraad, die handelt binnen de grenzen van de hem door de Overeenkomst verleende bevoegdheden." Artikel 12 luidt:

"De Overeenkomstsluitende Partijen komen overeen zich te laten leiden door de artikelen 48, 49 en 50 van het Verdrag tot oprichting van de Europese Gemeenschap, ten einde onderling geleidelijk het vrij verkeer van werknemers tot stand te brengen."

Aanvullend Protocol

Artikel 36 luidt:

"Het vrije verkeer van werknemers tussen de Lid-Staten van de Gemeenschap en Turkije wordt geleidelijk tot stand gebracht overeenkomstig de in artikel 12 van de Associatieovereenkomst neergelegde beginselen, tussen het einde van het twaalfde en het tweeëntwintigste jaar na de inwerkingtreding van genoemde Overeenkomst.

De hiertoe nodige regels worden door de Associatieraad bepaald."

Besluit nr. 2/76

Artikel 1 luidt:

"1. In het besluit wordt de wijze van toepassing van de tenuitvoerlegging van artikel 36 van het Aanvullend Protocol voor een eerste etappe vastgesteld.

2. De duur van deze eerste etappe is bepaald op vier jaar, ingaande op 1 december 1976."

Artikel 7 luidt:

"De Lid-Staten van de Gemeenschap en Turkije mogen geen nieuwe beperkingen invoeren met betrekking tot de toegang tot de werkgelegenheid van werknemers en hun gezinsleden wier verblijf en arbeid op hun onderscheiden grondgebied legaal zijn."

Artikel 13 luidt:

"Dit besluit treedt in werking op 20 december 1976."

Besluit nr. 1/80

Artikel 10 luidt:

"1. De Lid-Staten van de Gemeenschap passen op de Turkse werknemers die tot hun legale arbeidsmarkt behoren een stelsel toe dat wordt gekenmerkt door het ontbreken van elke discriminatie uit hoofde van de nationaliteit ten opzichte van communautaire werknemers, voor wat betreft de lonen en verdere arbeidsvoorwaarden.

[...]."

Artikel 13 luidt:

"De Lid-Staten van de Gemeenschap en Turkije mogen geen nieuwe beperkingen invoeren met betrekking tot de toegang tot de werkgelegenheid van werknemers en hun gezinsleden wier verblijf en arbeid op hun onderscheiden grondgebied legaal zijn."

Artikel 16 luidt:

"1. De bepalingen van dit deel zijn van toepassing met ingang van 1 december 1980."

[...]."

EU Handvest

Artikel 7 ("De eerbiediging van het privé-leven en van het familie- en gezinsleven") luidt:

"Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie."

Artikel 8 ("De bescherming van persoonsgegevens") luidt:

"1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd."

Artikel 51 ("Toepassingsgebied") luidt:

"1. De bepalingen van dit Handvest zijn gericht tot de instellingen, organen en instanties van de Unie met inachtneming van het subsidiariteitsbeginsel, alsmede, uitsluitend wanneer zij het recht van de Unie ten uitvoer brengen, de lidstaten. [...]."

Artikel 52 ("Reikwijdte van de gewaarborgde rechten") luidt:

"1. Beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

[...].

3. Voor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt. [...]."

Privacyrichtlijn

Artikel 1 ("Onderwerp van de richtlijn") luidt:

"1. De Lid-Staten waarborgen in verband met de verwerking van persoonsgegevens, overeenkomstig de bepalingen van deze richtlijn, de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer."

Artikel 2 ("Definities") luidt:

"In de zin van deze richtlijn wordt verstaan onder:

a) „persoonsgegevens”, iedere informatie betreffende een geïdentificeerde of

identificeerbare natuurlijke persoon, hierna „betrokkene" te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit;

b) „verwerking van persoonsgegevens", hierna „verwerking" te noemen, elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

c) „bestand van persoonsgegevens", hierna „bestand" te noemen, elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd dan wel gedecentraliseerd is of verspreid op een functioneel of geografisch bepaalde wijze; [...]."

Artikel 3 ("Werkingssfeer") luidt:

"1. De bepalingen van deze richtlijn zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

— die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat (waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van Staatsveiligheid), en de activiteiten van de Staat op strafrechtelijk gebied;

— die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht."

Artikel 6 luidt:

"1. De Lid-Staten bepalen dat de persoonsgegevens:

[...];

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet als onverenigbaar beschouwd, mits de Lid-Staten passende garanties bieden;

c) toereikend, ter zake dienend en niet bovenmatig moeten zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt;

[...];

e) in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is. De Lid-Staten voorzien in passende waarborgen voor persoonsgegevens die langer dan hierboven bepaald voor historische, statistische of wetenschappelijke doeleinden worden bewaard. [...]."

Artikel 7 luidt:

"1. De Lid-Staten bepalen dat de verwerking van persoonsgegevens slechts mag geschieden indien:

[...];

e) de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen, [...]."

Artikel 8 ("Verwerkingen die bijzondere categorieën gegevens betreffen") luidt:

"1. De Lid-Staten verbieden de verwerking van persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen.

2. Lid 1 is niet van toepassing wanneer:

a) de betrokkene uitdrukkelijk heeft toegestemd in een dergelijke verwerking, tenzij in de wetgeving van de Lid-Staat is bepaald dat het in lid 1 bedoelde verbod niet door toestemming van de betrokkene ongedaan kan worden gemaakt; of

b) de verwerking noodzakelijk is met het oog op de uitvoering van de verplichtingen en de rechten van de voor de verwerking verantwoordelijke inzake arbeidsrecht, voor zover zulks is toegestaan bij de nationale wetgeving en deze adequate garanties biedt; of

c) de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere persoon indien deze lichamelijk of juridisch niet in staat is van zijn instemming te getuigen; of

d) de verwerking wordt verricht door een stichting, een vereniging, of enige andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van hun gerechtvaardigde activiteiten en met de nodige garanties, mits de verwerking uitsluitend betrekking heeft op de leden van de stichting, de vereniging of de instantie of op de personen die in verband met haar streefdoelen regelmatige contacten met haar onderhouden, en de gegevens niet zonder de toestemming van de betrokkenen aan derden worden doorgegeven; of

e) de verwerking betrekking heeft op gegevens die duidelijk door de betrokkene openbaar zijn gemaakt of noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

[...].

4. Mits passende waarborgen worden geboden, mogen de Lid-Staten om redenen van zwaarwegend algemeen belang bij nationale wet of bij een besluit van de toezichthoudende

autoriteit nog andere afwijkingen naast die bedoeld in lid 2 vaststellen. [...]."
Verordening (EG) nr. 1030/2002

Punten 5 en 6 van de considerans luiden:

"5. Het is van wezenlijk belang dat het uniforme model voor verblijfstitels alle noodzakelijke gegevens bevat en aan zeer hoge technische normen voldoet, in het bijzonder met betrekking tot de garanties tegen namaak en vervalsing; dit zal bijdragen tot de doelstelling illegale immigratie en illegaal verblijf te verhinderen en te bestrijden. [...].

6. Om de bescherming tegen namaak en vervalsing te versterken, onderzoeken de lidstaten en de Commissie regelmatig, rekening houdend met de technologische ontwikkeling, welke veranderingen moeten worden aangebracht in de veiligheidselementen die in de titel zijn opgenomen, met name wat betreft de opnemings- en het gebruik van nieuwe biometrische kenmerken en methodes."

Artikel 1 luidt:

"1. De verblijfstitels die de lidstaten aan onderdanen van derde landen verstrekken, beantwoorden aan een uniform model en bieden ruimte voor de in de bijlage vermelde informatie. [...].

"2. Voor de toepassing van deze verordening wordt verstaan onder:

a) „verblijfstitel”: iedere door de autoriteiten van een lidstaat aan een onderdaan van een derde land verstrekte vergunning om legaal op zijn grondgebied te verblijven, behalve:

i) visa;

ii) titels die worden verstrekt hangende de behandeling van een asielaanvraag of van een verzoek om een verblijfstitel of een verzoek om verlenging daarvan;

ii bis) in uitzonderlijke gevallen afgegeven titels voor de verlenging van het toegestane verblijf met ten hoogste één maand;

iii) vergunningen die worden verstrekt voor een verblijf van ten hoogste zes maanden door de lidstaten die artikel 21 van de Overeenkomst ter uitvoering van het te Schengen gesloten akkoord van 14 juni 1985 tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen (9) niet toepassen; [...]."

Artikel 2 luidt:

"1. Overeenkomstig de in artikel 7, lid 2, bedoelde procedure worden aanvullende technische specificaties voor het uniforme model voor verblijfstitels vastgesteld voor:

a) de aanvullende elementen en vereisten inzake beveiliging, met inbegrip van hogere normen ter voorkoming van vervalsing en namaak;

[...].

d) de technische specificaties voor het opslagmedium van de biometrische kenmerken en de beveiliging daarvan, inclusief het beletten van ongeoorloofde toegang;

e) de kwaliteitsnormen en gemeenschappelijke normen inzake gezichtsopname en vingerafdrukbeelden;

[...]."

Artikel 3 luidt:

"In overeenstemming met de procedure bedoeld in artikel 7, lid 2, kan worden besloten dat de in artikel 2 bedoelde specificaties geheim moeten blijven en niet bekend worden gemaakt. [...]."

Artikel 4 luidt:

"[...].

Voor de toepassing van deze verordening mogen biometrische kenmerken in verblijfstitels alleen worden gebruikt voor het verifiëren van:

- a) de authenticiteit van het document;
- b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken indien de nationale wetgeving het overleggen van een verblijfstitel vereist."

Artikel 4 bis luidt:

"De uniforme verblijfstitel bevat een opslagmedium met de gezichtsopname en twee vingerafdrukbeelden van de houder, beide in een interoperabel formaat. De gegevens worden beveiligd en het opslagmedium heeft voldoende capaciteit en is voldoende geschikt om de integriteit, de authenticiteit en de vertrouwelijkheid van de gegevens te garanderen."

Artikel 4 ter luidt:

"Voor de toepassing van deze verordening, nemen de lidstaten biometrische identificatiemiddelen, waaronder de gezichtsopname en twee vingerafdrukken van onderdanen van derde landen.

[...].

De volgende biometrische identificatiemiddelen worden verzameld:

- een foto, die door de aanvrager wordt verstrekt of op het ogenblik van de aanvraag wordt gemaakt, en
- twee digitaal vastgelegde platte vingerafdrukken.

De technische specificaties voor het verzamelen van biometrische identificatiemiddelen worden vastgesteld overeenkomstig de procedure omschreven in artikel 7, lid 2, de normen van de ICAO, en de technische eisen voor de paspoorten die door de lidstaten overeenkomstig Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten aan hun onderdanen worden afgegeven.

Het nemen van vingerafdrukken is verplicht vanaf de leeftijd van zes jaar. Personen bij wie het nemen van vingerafdrukken fysiek onmogelijk is, worden vrijgesteld van de verplichting om vingerafdrukken te laten afnemen."

SIS II

Punten 10 tot en met 12 van de considerans luiden:

"10. SIS II moet signaleringen bevatten met het oog op weigering van toegang of verblijf. Het

beraad over de harmonisatie van de bepalingen inzake de gronden voor signaleringen van onderdanen van derde landen met het oog op weigering van toegang of verblijf en over de verduidelijking van het gebruik daarvan in het kader van het asiel-, immigratie- en terugkeerbeleid, moet worden voortgezet. [...].

11. Signaleringen met het oog op weigering van toegang of verblijf mogen niet langer in SIS II worden bewaard dan nodig is voor het bereiken van het doel waarvoor ze worden verstrekt. In de regel moeten zij na drie jaar automatisch uit SIS II worden verwijderd. Een besluit tot bewaring van de signalering gedurende een langere periode dient gebaseerd te zijn op een uitvoerige individuele beoordeling. De lidstaten moeten deze signaleringen binnen deze periode van drie jaar controleren en statistieken bijhouden betreffende het aantal signaleringen waarvan de bewaringstermijn is verlengd.

12. SIS II moet de verwerking van biometrische gegevens mogelijk maken om de betrouwbare identificatie van de betrokken personen te vergemakkelijken. In dit verband moet SIS II ook de verwerking mogelijk maken van gegevens van personen wier identiteit onrechtmatig is aangenomen, om problemen als gevolg van een verkeerde identificatie te voorkomen; daarbij moeten passende waarborgen worden geboden, met name de instemming van de betrokken persoon en een strikte beperking van de doeleinden waarvoor dergelijke gegevens rechtmatig kunnen worden verwerkt."

Artikel 1 ('Instelling en algemene doelstelling van SIS II') luidt:

"[...].

2. SIS II heeft tot doel, overeenkomstig het bepaalde in deze verordening, met behulp van de via dit systeem verstrekte informatie een hoog niveau van veiligheid te garanderen in een ruimte van vrijheid, veiligheid en rechtvaardigheid in de Europese Unie, onder meer door handhaving van de openbare orde en veiligheid en vrijwaring van de veiligheid op het grondgebied van de lidstaten, en de bepalingen inzake het personenverkeer op hun grondgebied van titel IV van het Verdrag toe te passen."

Artikel 2 ("Toepassingsgebied") luidt:

"1. In deze verordening worden de voorwaarden en procedures vastgesteld voor het opnemen en de verwerking van in SIS II opgenomen signaleringen in verband met onderdanen van derde landen, en voor de uitwisseling van aanvullende informatie en extra gegevens met het oog op weigering van toegang tot of verblijf op het grondgebied van de lidstaten.

[...]."

Artikel 20 ("Categorieën gegevens") luidt:

"1. Onverminderd artikel 8, lid 1, en de bepalingen van deze verordening met betrekking tot de opslag van aanvullende gegevens, bevat SIS II alleen de door elk van de lidstaten verstrekte categorieën gegevens, als vereist voor de in artikel 24 genoemde doeleinden.

2. Voor gesignaleerde personen worden ten hoogste de onderstaande gegevens opgenomen:

[...];

e) foto's;

f) vingerafdrukken;

[...]."

Artikel 21 ("Evenredigheidsbepaling") luidt:

Voorafgaand aan een signalering gaat een lidstaat na of de gepastheid, de relevantie en het belang van de zaak opnemend van de signalering in SIS II rechtvaardigen.

Artikel 24 ("Voorwaarden voor signaleringen met het oog op weigering van toegang of verblijf") luidt:

"1. Gegevens over met het oog op weigering van toegang of verblijf gesignaleerde onderdanen van derde landen worden opgenomen op grond van een nationale signalering ingevolge een door de bevoegde administratieve of strafrechtelijke autoriteiten met inachtneming van de nationale wettelijke procedurevoorschriften gegeven beslissing, op basis van een individuele beoordeling. Het recht van beroep tegen deze beslissingen wordt uitgeoefend overeenkomstig de nationale wetgeving.

2. Indien de in lid 1 bedoelde beslissing gegrond is op een gevaar voor de openbare orde of veiligheid of de nationale veiligheid dat de aanwezigheid van een onderdaan van een derde land op het grondgebied van een lidstaat kan opleveren, wordt een signalering opgenomen. Dit is in het bijzonder het geval bij:

a) een onderdaan van een derde land die in een lidstaat schuldig is bevonden aan een strafbaar feit waarvoor een vrijheidsstraf van ten minste één jaar geldt;

b) een onderdaan van een derde land te wiens aanzien er gegronde redenen zijn om aan te nemen dat hij ernstige misdrijven heeft gepleegd, of er duidelijke aanwijzingen zijn dat hij overweegt dergelijke feiten te plegen op het grondgebied van een lidstaat.

3. Een signalering kan tevens worden opgenomen indien de in lid 1 bedoelde beslissing gegrond was op het feit dat ten aanzien van de onderdaan van een derde land een niet-opgeschorte of niet-ingetrokken maatregel tot verwijdering, weigering van toegang of uitzetting is genomen die een verbod op binnenkomst, of, voor zover van toepassing, een verbod op verblijf behelst of daarvan vergezeld gaat, in verband met een overtreding van de nationale bepalingen inzake de binnenkomst en het verblijf van onderdanen van derde landen.

[...]."

Artikel 29 ("Termijn van bewaring van signaleringen") luidt:

"1. De in SIS II overeenkomstig deze verordening opgenomen signaleringen worden niet langer bewaard dan nodig is voor het nagestreefde doel.

2. Uiterlijk drie jaren na de opnemend van zo'n signalering in SIS II, toetst de signalerende lidstaat de noodzaak van verdere bewaring.

3. Elke lidstaat stelt in voorkomend geval volgens zijn nationale recht kortere toetsingstermijnen vast.

4. Een signalerende lidstaat kan, op grond van een uitvoerige individuele beoordeling, die schriftelijk wordt vastgelegd, vóór het verstrijken van de toetsingstermijn tot verdere bewaring van een signalering besluiten indien dit voor het met de signalering nagestreefde doel vereist is. In dat geval is lid 2 van toepassing op verlenging. Elke verlenging van een signalering wordt aan CS-SIS meegedeeld.

5. Na afloop van de in lid 2 bedoelde toetsingstermijn worden signaleringen automatisch gewist, behalve wanneer de signalerende lidstaat de verlenging van de signalering aan CS-SIS heeft meegedeeld, overeenkomstig lid 4. CS-SIS stelt de lidstaten vier maanden op voorhand automatisch in kennis van de in het systeem geprogrammeerde verwijdering.

6. De lidstaten houden statistieken bij van het aantal signaleringen waarvan de bewaring overeenkomstig lid 4 is verlengd."

VIS-verordening

Punten 5, 10 en 14 van de considerans luiden:

"5. Het VIS dient ten doel te hebben het verbeteren van de uitvoering van het gemeenschappelijk visumbeleid, de consulaire samenwerking en de raadpleging van de centrale visumautoriteiten, door de uitwisseling van gegevens betreffende aanvragen en de daarmee samenhangende beslissingen tussen de lidstaten te vergemakkelijken, teneinde de visumaanvraagprocedures te vergemakkelijken, „visumshopping" te voorkomen en fraudebestrijding en controles aan de doorlaatposten aan de buitengrenzen en op het grondgebied van de lidstaten te vergemakkelijken. Het VIS dient ook bij te dragen aan de identificatie van personen die niet of niet meer voldoen aan de voorwaarden voor binnenkomst, verblijf of vestiging op het grondgebied van de lidstaten, de toepassing van Verordening (EG) nr. 343/2003 en het voorkomen van bedreigingen van de binnenlandse veiligheid in de lidstaten.

10. Teneinde een betrouwbare verificatie en identificatie van visumaanvragers mogelijk te maken, moeten biometrische gegevens in het VIS worden verwerkt.

14. De in het VIS opgeslagen persoonsgegevens mogen niet langer worden bewaard dan voor de doelstellingen van het VIS noodzakelijk is. Het is aangewezen de gegevens gedurende een periode van ten hoogste vijf jaar te bewaren, zodat bij de beoordeling van visumaanvragen rekening kan worden gehouden met in eerdere aanvragen verstrekte gegevens, inclusief de goede trouw van de aanvragers, en met het oog op de registratie van illegale immigranten die wellicht ooit een visum hebben aangevraagd. Een kortere periode zou voor deze doelstellingen niet toereikend zijn. De gegevens moeten na afloop van de periode van vijf jaar worden verwijderd, tenzij er gronden zijn om dat eerder te doen."

Artikel 2 ("Doelstelling") luidt als volgt:

"Het VIS heeft ten doel de uitvoering van het gemeenschappelijk visumbeleid, de consulaire samenwerking en de raadpleging van de centrale visumautoriteiten te verbeteren door de uitwisseling van gegevens tussen de lidstaten betreffende aanvragen en de daarmee samenhangende beslissingen te vergemakkelijken, teneinde:

[...];;

c) fraudebestrijding te vergemakkelijken;

[...];

e) te helpen bij de identificatie van personen die niet of niet langer aan de voorwaarden voor binnenkomst, verblijf of vestiging op het grondgebied van de lidstaten voldoen;

f) de toepassing van Verordening (EG) nr. 343/2003 te vergemakkelijken;

g) bij te dragen tot het voorkomen van bedreigingen van de binnenlandse veiligheid van een

van de lidstaten."

Artikel 5 ("Categorieën gegevens") luidt als volgt:

"1. Alleen de volgende categorieën gegevens worden in het VIS opgeslagen:

[...];

b) foto's als bedoeld in artikel 9, lid 5;

c) vingerafdrukgegevens als bedoeld in artikel 9, lid 6;

[...]."

Artikel 23 ("Bewaringstermijn van opgeslagen gegevens") luidt als volgt:

"1. Onverminderd de verwijdering van gegevens als bedoeld in de artikelen 24 en 25 en de registratie van gegevens als bedoeld in artikel 34, worden de aanvraagdossiers voor ten hoogste vijf jaar in het VIS opgeslagen.

Deze termijn gaat in:

a) op de datum waarop de geldigheidsduur van het visum verstrijkt, indien een visum is afgegeven;

b) op de nieuwe datum waarop de geldigheidsduur van het visum verstrijkt, indien een visum is verlengd;

c) op de datum waarop het aanvraagdossier in het VIS is aangemaakt, indien de aanvraag ingetrokken, afgesloten of afgebroken is;

d) op de datum van de beslissing van de visumautoriteit dat het visum is geweigerd, dat het nietig is verklaard, of dat het is ingetrokken.

2. Na het verstrijken van de in lid 1 bedoelde termijn worden het aanvraagdossier en de in artikel 8, leden 3 en 4, bedoelde koppelingen naar dit dossier automatisch uit het VIS verwijderd."

Artikel 24 ("Wijziging van gegevens") luidt als volgt:

"1. Alleen de bevoegde lidstaat is gerechtigd om de gegevens welke die lidstaat aan het VIS heeft toegezonden, te wijzigen, door de gegevens te corrigeren of te verwijderen.

2. Indien een lidstaat over aanwijzingen beschikt dat in het VIS verwerkte gegevens onjuist zijn of dat gegevens in strijd met deze verordening in het VIS zijn verwerkt, stelt die lidstaat de bevoegde lidstaat daarvan onmiddellijk in kennis. Een dergelijke kennisgeving kan via de infrastructuur van het VIS worden toegezonden.

3. De bevoegde lidstaat controleert de betrokken gegevens en, indien nodig, corrigeert of verwijdert deze onmiddellijk."

Artikel 25 ("Vervroegde gegevensverwijdering") luidt als volgt:

"1. Indien voor het verstrijken van de in artikel 23, lid 1, bedoelde termijn een aanvrager de nationaliteit van een lidstaat heeft verworven, worden de aanvraagdossiers en de in artikel 8, leden 3 en 4, bedoelde koppelingen betreffende hem of haar door de lidstaat die het betrokken aanvraagdossier en de verbindingen heeft aangemaakt, onmiddellijk uit het VIS verwijderd.

2. Indien een aanvrager de nationaliteit van een lidstaat heeft verkregen, stelt die lidstaat de bevoegde lidstaat/lidstaten onverwijld daarvan in kennis. Een dergelijke kennisgeving kan via de infrastructuur van het VIS worden toegezonden. [...]."

VIS-Besluit

Punt 5 van de considerans luidt:

"Dit besluit is een aanvulling op Verordening (EG) nr. 767/2008

(VIS-verordening), omdat het een rechtsgrond in het kader van titel VI van het Verdrag betreffende de Europese Unie biedt voor toegang tot het VIS voor aangewezen autoriteiten en voor Europol.

Artikel 2 ("Definities") luidt als volgt:

"1. In dit besluit wordt verstaan onder:

[...];

c) „terroristische misdrijven”: strafbare feiten naar nationaal recht die overeenkomen met of gelijkwaardig zijn aan de strafbare feiten die zijn bedoeld in de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding;

d) „ernstige strafbare feiten”: de vormen van criminaliteit die overeenkomen met of gelijkwaardig zijn aan de strafbare feiten bedoeld in artikel 2, lid 2, van Kaderbesluit 2002/584/JBZ;

[...]."

Artikel 5 ("Voorwaarden voor toegang tot het VIS door de aangewezen autoriteiten van de lidstaten") luidt als volgt:

"1. Toegang tot het VIS voor raadpleging door aangewezen autoriteiten is alleen mogelijk binnen het kader van de bevoegdheden van die autoriteiten en indien aan de volgende voorwaarden is voldaan:

a) toegang voor raadpleging moet noodzakelijk zijn voor het voorkomen, opsporen of onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten;

b) toegang voor raadpleging moet noodzakelijk zijn in een specifiek geval;

c) er bestaan gegronde redenen om aan te nemen dat raadpleging van de VIS-gegevens wezenlijk bijdraagt tot het voorkomen, opsporen of onderzoeken van een van de betrokken strafbare feiten.

[...]."

Visumcode

Artikel 10 ("Algemene voorschriften voor het indienen van een aanvraag") luidt als volgt:

"1. Onverminderd de bepalingen van de artikelen 13, 42, 43 en 45, dient de aanvrager, bij het indienen van een aanvraag, in persoon te verschijnen.

[...].

3. Bij het indienen van de aanvraag moet de aanvrager:

[...];

c) een foto overleggen die beantwoordt aan de normen van Verordening (EG) nr. 1683/95 of, indien het VIS operationeel is overeenkomstig artikel 48 van de VIS-verordening, die beantwoordt aan de in artikel 13 van deze verordening vastgestelde normen;

d) de afname van zijn vingerafdrukken toestaan overeenkomstig artikel 13, voor zover van toepassing;

[...]."

Artikel 13 ("Biometrische kenmerken") luidt als volgt:

"1. De lidstaten verzamelen biometrische kenmerken van de aanvrager, omvattende diens gezichtsoptname en tien vingerafdrukken, overeenkomstig de waarborgen vastgelegd in het Verdrag van de Raad van Europa tot bescherming van de rechten van de mens en de fundamentele vrijheden, het Handvest van de grondrechten van de Europese Unie en het VN-Verdrag inzake de rechten van het kind.

2. Bij de indiening van de eerste aanvraag dient de aanvrager persoonlijk te verschijnen. Op dat ogenblik worden de volgende biometrische kenmerken van de aanvrager verzameld

— een gescande of op het ogenblik van de aanvraag genomen foto, en

— tien vlak afgenomen en digitaal verzamelde vingerafdrukken.

3. Indien de bij een voorgaande aanvraag van de aanvrager genomen vingerafdrukken minder dan 59 maanden vóór de datum van de nieuwe aanvraag voor het eerst in het VIS werden opgenomen, worden zij naar de volgende aanvraag gekopieerd.

[...].

7. De volgende aanvragers worden vrijgesteld van de verplichte afgifte van vingerafdrukken:

a) kinderen jonger dan twaalf jaar;

b) personen bij wie het nemen van vingerafdrukken fysiek onmogelijk is. Indien het mogelijk is vingerafdrukken te nemen, ook al zijn het er minder dan tien, dan moet het maximale aantal vingerafdrukken worden genomen. Gaat het evenwel om een tijdelijke onmogelijkheid, dan moeten van de aanvrager bij de volgende aanvraag vingerafdrukken worden genomen.

De krachtens artikel 4, leden 1, 2 en 3, bevoegde autoriteiten mogen om nadere verduidelijking betreffende de redenen voor de tijdelijke onmogelijkheid verzoeken. De lidstaten zorgen ervoor dat er passende procedures zijn ter waarborging van de waardigheid van de aanvrager in het geval dat er moeilijkheden zijn bij het opnemen van de gegevens;

[...]."

Eurodac-verordening

De punten 4 tot en met 6, 8, 10, 15 en 22 van de considerans luiden:

"4. Voor de toepassing van Verordening (EU) nr. 604/2013 [...], is het noodzakelijk de identiteit vast te stellen van personen die om internationale bescherming verzoeken en van personen die in verband met de onrechtmatige overschrijding van de buitengrens van de Unie zijn aangehouden. Tevens is het met het oog op een doeltreffende toepassing van Verordening (EU) nr. 604/2013, en met name van artikel 18, lid 1, onder b) en d), wenselijk elke lidstaat de mogelijkheid te bieden na te gaan of een onderdaan van een derde land of

een staatloze die illegaal op zijn grondgebied verblijft, in een andere lidstaat om internationale bescherming heeft verzocht.

5. Vingerafdrukken vormen een belangrijk element om de juiste identiteit van die personen vast te stellen, hetgeen ertoe noopt een systeem voor de vergelijking van hun vingerafdrukgegevens in te stellen.

6. Daartoe is het noodzakelijk om een systeem op te zetten, "Eurodac" genaamd, bestaande uit een centraal systeem dat een geautomatiseerde centrale gegevensbank van vingerafdrukgegevens beheert, [...].

8. Het is voor de bestrijding van terroristische misdrijven en andere ernstige strafbare feiten van wezenlijk belang dat de rechtshandavingsinstanties over zoveel mogelijk actuele informatie beschikken om hun taken uit te voeren. De in Eurodac opgenomen gegevens zijn noodzakelijk voor het voorkomen, opsporen of onderzoeken van terroristische misdrijven als bedoeld in Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding of andere ernstige strafbare feiten als bedoeld in Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten. Daarom dienen de gegevens in Eurodac onder de in deze verordening vastgestelde voorwaarden beschikbaar te zijn voor vergelijking door de aangewezen autoriteiten van de lidstaten en de Europese Politiedienst (Europol).

10. In haar mededeling aan de Raad en het Europees Parlement van 24 november 2005 over de verbetering van de doeltreffendheid, de interoperabiliteit en de synergie van de Europese gegevensbanken op het gebied van justitie en binnenlandse zaken heeft de Commissie uiteengezet dat de binnenlandse veiligheidsinstanties in welbepaalde gevallen toegang tot Eurodac zouden kunnen krijgen, wanneer er een geground vermoeden bestaat dat iemand die een terroristisch of ander ernstig strafbaar feit heeft gepleegd, om internationale bescherming heeft verzocht. In die mededeling stelde de Commissie ook dat het evenredigheidsbeginsel vereist dat Eurodac alleen voor deze doeleinden kan worden geraadpleegd als er sprake is van een doorslaggevend openbaarveiligheidsbelang, dat wil zeggen als het door de te identificeren crimineel of terrorist gepleegde feit zo laakbaar is dat het gerechtvaardigd is een gegevensbank te raadplegen waarin personen zonder strafblad worden geregistreerd, en besloot zij dat de drempel om Eurodac te raadplegen voor binnenlandse veiligheidsinstanties dan ook altijd aanzienlijk hoger dient te liggen dan die voor het raadplegen van strafrechtelijke gegevensbanken.

15. In deze verordening worden ook de voorwaarden vastgesteld waaronder verzoeken om vergelijking van vingerafdrukgegevens met Eurodac-gegevens mogelijk dienen te zijn om terroristische misdrijven of andere ernstige strafbare feiten te voorkomen, op te sporen of te onderzoeken alsook de noodzakelijke waarborgen ter bescherming van het grondrecht op eerbiediging van het privéleven van personen van wie de persoonsgegevens in Eurodac worden verwerkt. Deze voorwaarden zijn streng omdat in de Eurodac-gegevensbank vingerafdrukgegevens worden geregistreerd van personen die er niet van worden verdacht een terroristisch misdrijf of ander ernstig strafbaar feit te hebben gepleegd.

22. Onderdanen van derde landen of staatlozen die in één lidstaat om internationale bescherming hebben verzocht, kunnen nog tal van jaren over de mogelijkheid beschikken om dat ook in een andere lidstaat te doen. Daarom moet het maximale tijdsbestek gedurende hetwelk vingerafdrukken door het centraal systeem dienen te worden bewaard, vrij lang zijn. Gezien het feit dat de meeste onderdanen van derde landen of staatlozen die een aantal jaren in de Unie hebben verbleven, na die periode een vaste status of zelfs het burgerschap van

een lidstaat hebben verkregen, dient een periode van tien jaar voor de bewaring van vingerafdrukgegevens als een redelijke termijn te worden beschouwd."

Artikel 2 ("Definities") luidt als volgt:

"1. Voor de doeleinden van deze verordening wordt verstaan onder:

a) "persoon die om internationale bescherming verzoekt": een onderdaan van een derde land of een staatloze die een verzoek om internationale bescherming in de zin van artikel 2, onder h) van Richtlijn 2011/95/EU heeft ingediend waarover nog geen definitieve beslissing is genomen;

[...].

i) "rechtshandhaving": de preventie, de opsporing of het onderzoek van terroristische misdrijven of van andere ernstige strafbare feiten;

j) "terroristische misdrijven": strafbare feiten naar nationaal recht die overeenkomen met of gelijkwaardig zijn aan de strafbare feiten bedoeld in de artikelen 1 tot en met 4 van Kaderbesluit 2002/475/JBZ;

k) "ernstige strafbare feiten": de vormen van criminaliteit die overeenkomen met of gelijkwaardig zijn aan de strafbare feiten bedoeld in artikel 2, lid 2, van Kaderbesluit 2002/584/JBZ, die volgens het nationale recht strafbaar zijn gesteld met een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel met een maximumduur van ten minste drie jaar;

[...]."

Artikel 9 ("Verzameling, toezending en vergelijking van vingerafdrukken") luidt als volgt:

"1. Elke lidstaat neemt onverwijld de vingerafdrukken van alle vingers van elke persoon van 14 jaar of ouder die om internationale bescherming verzoekt en zendt deze samen met de in artikel 11, onder b) tot en met g), van deze verordening genoemde gegevens zo spoedig mogelijk en uiterlijk 72 uur na de indiening van zijn verzoek om internationale bescherming in de zin van artikel 20, lid 2, van Verordening (EU) nr. 604/2013, toe aan het centraal systeem."

[...]."

Artikel 11 ("Opslag van gegevens") luidt als volgt:

"1. Slechts de volgende gegevens worden in het centraal systeem vastgelegd:

a) vingerafdrukgegevens;

[...]."

Artikel 12 ("Bewaring van gegevens") luidt als volgt:

"1. Elke reeks gegevens als vermeld in artikel 11 wordt in het centraal systeem bewaard voor een periode van tien jaar vanaf de datum waarop de vingerafdrukken zijn genomen.

2. Na het verstrijken van de in lid 1 bedoelde periode worden de gegevens automatisch door het centraal systeem uit het centraal systeem verwijderd."

Artikel 13 ("Eerder verwijderen van gegevens") luidt als volgt:

"1. Gegevens over een persoon die vóór het verstrijken van de in artikel 12 gestelde termijn

het burgerschap van een lidstaat heeft verkregen, worden in het centraal systeem verwijderd overeenkomstig artikel 27, lid 4, zodra de lidstaat van oorsprong er kennis van neemt dat de persoon in kwestie dat burgerschap heeft verkregen.
[...]."

Artikel 14 ("Verzamelen en toezenden van vingerafdrukgegevens") luidt als volgt:

"1. Elke lidstaat neemt onverwijld de vingerafdrukken van alle vingers van elke onderdaan van een derde land of staatloze van veertien jaar of ouder die, komende uit een derde land, door de bevoegde controleautoriteiten van een lidstaat is aangehouden in verband met het illegaal over land, over zee of door de lucht overschrijden van de grens van die lidstaat, en die niet is teruggezonden of die fysiek op het grondgebied van de lidstaten blijft en niet in afzondering of bewaring wordt gehouden gedurende de gehele periode tussen de aanhouding en de verwijdering op grond van de beslissing hem terug te zenden.

[...]."

Artikel 16 ("Bewaring van gegevens") luidt als volgt:

"1. Elke reeks gegevens over een onderdaan van een derde land of een staatloze als vermeld in artikel 14, lid 1, wordt in het centraal systeem bewaard voor een periode van achttien maanden, vanaf de datum waarop de vingerafdrukken van de onderdaan van een derde land of de staatloze zijn genomen. Daarna worden dergelijke gegevens automatisch uit het centraal systeem verwijderd.

2. De gegevens over een onderdaan van een derde land of een staatloze als bedoeld in artikel 14, lid 1, worden uit het centraal systeem verwijderd overeenkomstig artikel 28, lid 3, zodra de lidstaat van oorsprong vóór het verstrijken van de in lid 1 van dit artikel genoemde termijn van achttien maanden van één van de volgende omstandigheden kennis krijgt:

- a) de onderdaan van een derde land of de staatloze heeft een verblijfstitel gekregen;
- b) de onderdaan van een derde land of de staatloze heeft het grondgebied van de lidstaten verlaten;
- c) de onderdaan van een derde land of de staatloze heeft het burgerschap van een lidstaat verkregen.

[...]."

Artikel 20 ("Voorwaarden voor toegang tot Eurodac door de aangewezen autoriteiten") luidt als volgt:

"1. Met het oog op de in artikel 1, lid 2, vastgelegde doeleinden mogen aangewezen autoriteiten binnen het kader van hun bevoegdheden alleen een gemotiveerd elektronisch verzoek richten ter vergelijking van vingerafdrukgegevens met in het centraal systeem opgeslagen gegevens wanneer vergelijkingen met de onderstaande gegevensbanken niet tot de vaststelling van de identiteit van de betrokkene hebben geleid:

— nationale vingerafdrukgegevensbanken;

— de geautomatiseerde dactyloscopische identificatiesystemen van alle andere lidstaten op grond van Besluit 2008/615/JBZ indien vergelijkingen technisch beschikbaar zijn, tenzij er gegronde redenen bestaan om aan te nemen dat de vergelijking met dergelijke systemen niet tot de vaststelling van de identiteit van de betrokkene zou leiden. Die gegronde redenen

worden opgenomen in het gemotiveerde elektronische verzoek om vergelijking met Eurodac-gegevens dat de aangewezen autoriteit naar de controlerende autoriteit stuurt; en
— het Visuminformatiesysteem mits aan de in Besluit 2008/633/JBZ vermelde voorwaarden voor een dergelijke vergelijking is voldaan;

en indien aan elk van de volgende voorwaarden is voldaan:

a) de vergelijking is noodzakelijk voor het voorkomen, opsporen of onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten, wat betekent dat er sprake is van een doorslaggevend openbaarveiligheidsbelang dat het doorzoeken van de gegevensbank rechtvaardigt;

b) de vergelijking is noodzakelijk in een specifiek geval (wat inhoudt dat er geen systematische vergelijkingen worden verricht); en

c) er bestaan gegronde redenen om aan te nemen dat de vergelijking wezenlijk zal bijdragen tot het voorkomen, opsporen of onderzoeken van de betrokken strafbare feiten. Dergelijke gegronde redenen bestaan met name wanneer er een gegrond vermoeden bestaat dat de verdachte, de overtreder of het slachtoffer van een terroristisch misdrijf of een ander ernstig strafbaar feit behoort tot één van de in deze verordening behandelde categorieën."

Bijlage (in de Franse taal)

Le droit de l'Union Européenne

L'accord d'association

L'article 2 comme suit:

"1. L'accord a pour objet de promouvoir le renforcement continu et équilibré des relations commerciales et économiques entre les Parties, en tenant pleinement compte de la nécessité d'assurer le développement accéléré de l'économie de la Turquie et le relèvement du niveau de l'emploi et des conditions de vie du peuple turc.

[...]."

L'article 6 comme suit:

"Pour assurer l'application et le développement progressif du régime d'association, les Parties contractantes se réunissent au sein d'un Conseil d'association qui agit dans les limites des attributions qui lui sont conférées par l'accord [d'association]."

L'article 12 comme suit:

"Les Parties contractantes conviennent de s'inspirer des articles 48,49 et 50 du traité instituant la Communauté pour réaliser graduellement la libre circulation des travailleurs entre elles."

Le Protocole Additionnel

L'article 36 comme suit:

"La libre circulation des travailleurs entre les États membres de la Communauté et la Turquie sera réalisée graduellement conformément aux principes énoncés à l'article 12 de l'accord d'association, entre la fin de la douzième et de la vingt-deuxième année après l'entrée en

vigueur dudit accord.

Le Conseil d'association décidera des modalités nécessaires à cet effet."

La Décision n° 2/76

L'article 1 comme suit:

"1. La présente décision fixe, pour une première étape, les modalités de mise en oeuvre de l'article 36 du protocole additionnel.

2. La durée de cette première étape est fixée à quatre ans, à partir du 1er décembre 1976."

L'article 7 comme suit:

"Les Etats membres de la Communauté et la Turquie ne peuvent introduire de nouvelles restrictions concernant les conditions d'accès à l'emploi des travailleurs qui se trouvent sur leur territoire respectif en situation régulière en ce qui concerne leur séjour et leur emploi."

L'article 13 comme suit:

"La présente décision entre en vigueur le 20 décembre 1976."

La Décision n° 1/80

L'article 10 comme suit:

"1. Les États membres de la Communauté accordent aux travailleurs turcs appartenant à leur marché régulier de l'emploi un régime caractérisé par l'absence de toute discrimination fondée sur la nationalité par rapport aux travailleurs communautaires en ce qui concerne la rémunération et les autres conditions de travail.

[...]."

L'article 13 comme suit:

"Les États membres de la Communauté et la Turquie ne peuvent introduire de nouvelles restrictions concernant les conditions d'accès à l'emploi des travailleurs et des membres de leur famille qui se trouvent sur leur territoire respectif en situation régulière en ce qui concerne le séjour et l'emploi."

L'article 16 comme suit:

"1. Les dispositions de la présente section sont applicables à partir du 1er décembre 1980."

[...]."

Charte des Droits Fondamentaux de L'Union Européenne

L'article 7 ("Respect de la vie privée et familiale") comme suit:

"Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications."

L'article 8 ("Protection des données à caractère personnel") comme suit:

"1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu

par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante."

L'article 51 ("Champ d'application") comme suit:

"1. Les dispositions de la présente Charte s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en oeuvre le droit de l'Union. [...]."

L'article 52 ("Portée et interprétation des droits et des principes") comme suit:

"1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

[...].

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue. [...]."

Directive 95/46/CE

L'article 1 ("Objet de la directive") comme suit:

"1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel."

L'article 2 ("Définitions") comme suit:

"Aux fins de la présente directive, on entend par:

a) „données à caractère personnel": toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

b) „traitement de données à caractère personnel"(traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;

c) „fichier de données à caractère personnel" (fichier): tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique; [...]."

L'article 3 ("Champ d'application") comme suit:

"1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel:

— mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

— effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques."

L'article 6 comme suit:

"1. Les États membres prévoient que les données à caractère personnel doivent être:

[...];

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;

c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;

[...];

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques. [...]."

L'article 7 comme suit:

"Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si:

[...];

e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, [...]."

L'article 8 ("Traitements portant sur des catégories particulières de données") comme suit:

"1. Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la

santé et à la vie sexuelle .

2. Le paragraphe 1 ne s'applique pas lorsque:

- a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée; ou
- b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates; ou
- c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; ou
- d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées; ou
- e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

[...].

4. Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle. [...]."

Règlement (CE) No 1030/2002

Points 5 et 6 du préambule comme suit:

"5. Il est essentiel que le modèle uniforme de titre de séjour contienne toutes les informations nécessaires et qu'il réponde à des normes techniques de très haut niveau, notamment en ce qui concerne les garanties contre la contrefaçon et la falsification. Cela contribuera à la prévention de l'immigration clandestine et du séjour irrégulier et à la lutte contre ces phénomènes. Le modèle devrait aussi être adapté à son utilisation par tous les États membres et comporter des dispositifs de sécurité harmonisés, universellement reconnaissables, qui soient visibles à l'oeil nu.

6. Pour renforcer la protection des titres de séjour contre la contrefaçon et la falsification, les États membres et la Commission examinent à intervalles réguliers, au fur et à mesure de l'évolution technologique, les changements à apporter dans les éléments de sécurité incorporés dans le titre, et notamment l'intégration et l'utilisation de nouveaux éléments biométriques."

L'article 1 comme suit:

"1. Les titres de séjour délivrés par les États membres aux ressortissants des pays tiers sont établis selon un modèle uniforme et réservent un espace suffisant pour les informations mentionnées en annexe. [...].

2. Aux fins du présent règlement, on entend par:

a) „titre de séjour”: toute autorisation délivrée par les autorités d'un État membre et permettant à un ressortissant d'un pays tiers de séjourner légalement sur son territoire, à l'exception:

i) des visas;

ii) des titres délivrés pour la durée de l'instruction d'une demande d'asile, d'une demande de titre de séjour ou d'une demande de prolongation de celui-ci;

ii bis) des titres délivrés dans des circonstances exceptionnelles en vue d'une prolongation du séjour autorisé pour une durée maximale d'un mois;

iii) des autorisations délivrées pour un séjour dont la durée n'excède pas les six mois, par les États membres qui n'appliquent pas les dispositions de l'article 21 de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes; [...]."

L'article 2 comme suit:

"1. Des spécifications techniques complémentaires pour le modèle uniforme de titre de séjour sont établies, conformément à la procédure prévue à l'article 7, paragraphe 2, en ce qui concerne:

a) les éléments et les exigences de sécurité complémentaires, y compris des normes de prévention renforcées contre le risque de contrefaçon et de falsification;

[...].

d) les spécifications techniques relatives au support de stockage des éléments biométriques et à sa sécurisation, y compris la prévention de l'accès non autorisé;

e) les exigences de qualité et les normes communes en ce qui concerne l'image faciale et les images d'empreintes digitales;

[...]."

L'article 3 comme suit:

"Il peut être décidé, selon la procédure mentionnée à l'article 7, paragraphe 2, que les spécifications visées à l'article 2 sont secrètes et ne sont pas publiées. [...]."

L'article 4 comme suit:

"[...].

Aux fins du présent règlement, les éléments biométriques intégrés dans les titres de séjour ne sont utilisés que pour vérifier:

a) l'authenticité du document;

b) l'identité du titulaire grâce à des éléments comparables et directement disponibles lorsque la législation nationale exige la production du titre de séjour."

L'article 4 bis comme suit:

"Le modèle uniforme de titre de séjour comporte un support de stockage contenant une image faciale et deux images d'empreintes digitales du titulaire, ces images étant toutes enregistrées dans des formats interopérables. Les données sont sécurisées et le support de stockage est doté d'une capacité suffisante et présente les caractéristiques nécessaires pour garantir l'intégrité, l'authenticité et la confidentialité des données."

L'article 4 ter comme suit:

"Aux fins du présent règlement, les États membres relèvent les identificateurs biométriques, comprenant l'image faciale et deux empreintes digitales, des ressortissants de pays tiers.

[...].

Les identificateurs biométriques suivants sont collectés:

- une photographie fournie par le demandeur ou prise au moment de la demande, et
- deux empreintes digitales relevées à plat et numérisées.

Les spécifications techniques pour la collecte des identificateurs biométriques sont établies conformément à la procédure définie à l'article 7, paragraphe 2, et aux normes de l'OACI ainsi qu'aux spécifications techniques applicables aux passeports délivrés par les États membres à leurs ressortissants en vertu du règlement (CE) no 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

La saisie des empreintes digitales est obligatoire à partir de l'âge de six ans.

Les personnes dont il est physiquement impossible de relever les empreintes digitales sont exemptées de l'obligation de les donner."

SIS II

Points 10 à 12 du préambule comme suit:

"10. Le SIS contiendra des signalements aux fins de nonadmission ou d'interdiction de séjour. Il y a nécessité de continuer à envisager une harmonisation des dispositions relatives aux motifs justifiant l'introduction de signalements de ressortissants de pays tiers à des fins de nonadmission ou d'interdiction de séjour et de préciser leur utilisation dans le cadre des politiques en matière d'asile, d'immigration et de retour. En conséquence, la Commission devrait réexaminer, trois ans à compter de la date à partir de laquelle le présent règlement s'appliquera, les dispositions relatives aux objectifs des signalements introduits aux fins de nonadmission ou d'interdiction de séjour et aux conditions auxquelles ils sont soumis.

11. Les signalements aux fins de non-admission ou d'interdiction de séjour ne devraient pas être conservés dans le SIS II pour une durée plus longue que le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été fournis. En principe, ils devraient être automatiquement effacés du

SIS II après trois ans. Toute décision de conserver un signalement pour une plus longue période devrait se fonder sur une évaluation individuelle complète. Les États membres devraient réexaminer ces signalements dans ce délai de trois ans et tenir des statistiques concernant le nombre de signalements dont la durée de conservation a été prolongée.

12. Le SIS II devrait permettre le traitement des données biométriques afin d'aider à

l'identification correcte des personnes concernées. À cet égard, le SIS II devrait également permettre le traitement de données relatives à des personnes dont l'identité a été usurpée, de manière à éviter les problèmes que pourraient causer des erreurs d'identification, sous réserve de garanties adaptées, en particulier le consentement des personnes concernées et une stricte limitation des fins auxquelles ces données peuvent être licitement traitées."

L'article 1 ("Établissement et objectif général du SIS II") comme suit:

"[...].

2. L'objet du SIS II, conformément aux dispositions du présent règlement, est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que d'appliquer les dispositions du titre IV, chapitre 3, du traité relatives à la libre circulation des personnes sur les territoires des États membres, à l'aide des informations transmises par ce système."

L'article 2 ("Champ d'application") comme suit:

"1. Le présent règlement établit les conditions et les procédures relatives à l'introduction et au traitement dans le SIS II des signalements de ressortissants de pays tiers, ainsi qu'à l'échange d'informations supplémentaires et de données complémentaires aux fins de non-admission ou d'interdiction de séjour dans les États membres.

[...]."

L'article 20 ("Catégories de données") comme suit:

"1. Sans préjudice des dispositions de l'article 8, paragraphe 1, ou des dispositions du présent règlement prévoyant le stockage de données complémentaires, le SIS II contient exclusivement les catégories de données qui sont fournies par chacun des États membres et qui sont nécessaires aux fins prévues à l'article 24.

2. Les renseignements concernant les personnes signalées comprennent au maximum les éléments suivants:

[...];

e) les photographies;

f) les empreintes digitales;

[...]."

L'article 21 ("Proportionnalité") comme suit:

"Avant d'introduire un signalement, l'État membre signalant vérifie si le cas est suffisamment approprié, pertinent et important pour justifier l'introduction du signalement dans le SIS II."

L'article 24 ("Conditions auxquelles sont soumis les signalements introduits aux fins de nonadmission ou d'interdiction de séjour") comme suit:

"1. Les données relatives aux ressortissants de pays tiers faisant l'objet d'un signalement aux fins de non-admission ou d'interdiction de séjour sont introduites sur la base d'un signalement national résultant d'une décision prise par les autorités administratives ou juridictions compétentes dans le respect des règles de procédure prévues par la législation nationale, sur la base d'une évaluation individuelle. Les recours contre cette décision sont

formés conformément à la législation nationale.

2. Un signalement est introduit lorsque la décision visée au paragraphe 1 est fondée sur la menace pour l'ordre public ou la sécurité publique ou pour la sécurité nationale que peut constituer la présence d'un ressortissant d'un pays tiers sur le territoire d'un État membre. Tel peut être notamment le cas:

a) d'un ressortissant d'un pays tiers qui a été condamné dans un État membre pour une infraction passible d'une peine privative de liberté d'au moins un an;

b) d'un ressortissant d'un pays tiers à l'égard duquel il existe des raisons sérieuses de croire qu'il a commis un fait punissable grave, ou à l'égard duquel il existe des indices réels qu'il envisage de commettre un tel fait sur le territoire d'un État membre.

3. Un signalement peut également être introduit lorsque la décision visée au paragraphe 1 est fondée sur le fait que le ressortissant d'un pays tiers a fait l'objet d'une mesure d'éloignement, de renvoi ou d'expulsion qui n'a pas été abrogée ni suspendue, et qui comporte ou est assortie d'une interdiction d'entrée, ou, le cas échéant, de séjour, fondée sur le non-respect des réglementations nationales relatives à l'entrée ou au séjour des ressortissants de pays tiers.

[...]."

L'article 29 ("Durée de conservation des signalements") comme suit:

"1. Les signalements introduits dans le SIS II aux fins du présent règlement ne sont conservés que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits.

2. Dans les trois ans à compter de l'introduction d'un tel signalement dans le SIS II, l'État membre signalant examine la nécessité de le maintenir.

3. Chaque État membre fixe, le cas échéant, des délais d'examen plus courts, conformément à son droit national.

4. L'État membre signalant peut, dans le délai d'examen, décider, au terme d'une évaluation individuelle globale, qui est enregistrée, de maintenir le signalement si ce maintien est nécessaire aux fins qui sont à la base du signalement. Dans ce cas, le paragraphe 2 s'applique également à la prolongation. Toute prolongation du signalement doit être communiquée au CS-SIS.

5. Les signalements sont automatiquement effacés à l'expiration du délai d'examen visé au paragraphe 2, sauf dans le cas où l'État membre signalant a communiqué la prolongation du signalement au CS-SIS conformément au paragraphe 4. Le CS-SIS signale automatiquement aux États membres l'effacement programmé dans le système avec un préavis de quatre mois.

6. Les États membres tiennent des statistiques concernant le nombre de signalements dont la durée de conservation a été prolongée conformément au paragraphe 4."

Règlement VIS

Points 5, 10 et 14 du préambule comme suit:

"5. Le VIS devrait avoir pour objet d'améliorer la mise en oeuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités centrales chargées

des visas en facilitant l'échange de données entre les États membres sur les demandes de visas et les décisions y relatives, dans le but de simplifier les procédures de demande de visa, de prévenir le „visa shopping“, de faciliter la lutte contre la fraude et de faciliter les contrôles aux points de passage aux frontières extérieures et sur le territoire des États membres. Le VIS devrait également aider à l'identification de toute personne qui ne remplit pas ou ne remplit plus les conditions d'entrée, de présence ou de séjour applicables sur le territoire des États membres et faciliter l'application du règlement (CE) no 343/2003 du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers ainsi que contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des États membres.

10. Afin d'assurer une vérification et une identification fiables des demandeurs de visas, il est nécessaire de traiter des données biométriques dans le VIS.

14. Les données à caractère personnel enregistrées dans le VIS ne devraient pas être conservées plus longtemps que ce qui est nécessaire pour les besoins du VIS. Il est approprié de conserver les données pendant une période maximale de cinq ans, afin que les données relatives à des demandes

précédentes puissent être prises en considération pour évaluer des demandes de visas, y compris la bonne foi des demandeurs, et pour établir des dossiers sur les personnes en situation irrégulière qui peuvent avoir déposé une demande de visa à un moment donné. Une période plus courte ne serait pas suffisante à ces fins. Les données devraient être effacées après une période de cinq ans, à moins qu'il y ait des raisons de les effacer avant."

L'article 2 ("Objet") comme suit:

"Le VIS a pour objet d'améliorer la mise en oeuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités consulaires centrales chargées des visas en facilitant l'échange de données entre les États membres sur les demandes de visas et les décisions y relatives, dans le but de:

[...];

c) faciliter la lutte contre la fraude;

[...];

e) aider à l'identification de toute personne qui ne remplit pas ou ne remplit plus les conditions d'entrée, de présence ou de séjour sur le territoire des États membres;

f) faciliter l'application du règlement (CE) no 343/2003;

g) contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des États membres."

L'article 5 ("Catégories de données") comme suit:

"1. Seules les catégories de données suivantes sont enregistrées dans le VIS:

[...];

b) photographies visées à l'article 9, paragraphe 5;

c) empreintes digitales visées à l'article 9, paragraphe 6;

[...]."

L'article 23 ("Durée de conservation des données stockées) comme suit:

"1. Chaque dossier de demande est conservé dans le VIS pendant une période maximale de cinq ans, sans préjudice de l'effacement des données visé aux articles 24 et 25 et de l'établissement de relevés visé à l'article 34.

Cette période débute:

- a) à la date d'expiration du visa, en cas de délivrance d'un visa;
 - b) à la nouvelle date d'expiration du visa, en cas de prorogation d'un visa;
 - c) à la date de la création du dossier de demande dans le VIS, en cas de retrait, de clôture ou d'interruption de la demande;
 - d) à la date de la décision de l'autorité chargée des visas, en cas de refus, d'annulation, de réduction ou de retrait d'un visa.
2. À l'expiration de la période visée au paragraphe 1, le VIS efface automatiquement le dossier de demande et le(s) lien(s) s'y rapportant, conformément aux dispositions de l'article 8, paragraphes 3 et 4."

L'article 24 ("Modification des données") comme suit:

- "1. L'État membre responsable est seul habilité à modifier les données qu'il a transmises au VIS en les rectifiant ou en les effaçant.
2. Si un État membre dispose d'éléments tendant à démontrer que les données traitées dans le VIS sont erronées ou que leur traitement dans le VIS est contraire au présent règlement, il en informe immédiatement l'État membre responsable. Ce message peut être transmis par l'infrastructure du VIS.
3. L'État membre responsable vérifie les données en question et, au besoin, les rectifie ou les efface immédiatement."

L'article 25 ("Effacement anticipé des données") comme suit:

- "1. Les dossiers de demande et les liens visés à l'article 8, paragraphes 3 et 4, concernant un demandeur ayant acquis la nationalité d'un État membre avant l'expiration de la période visée à l'article 23, paragraphe 1, sont effacés du VIS sans délai par l'État membre responsable qui a créé le(s) dossier(s) de demande y relatif(s) et les liens.
2. Chaque État membre informe sans délai l'État membre (ou les États membres) responsable(s) de l'acquisition de sa nationalité par un demandeur. Ce message peut être transmis par l'infrastructure du VIS. [...]."

VIS Décision

Point 5 du préambule comme suit:

"5. La présente décision complète le règlement (CE) no 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (3), dans la mesure où elle fournit une base juridique dans le cadre du titre VI du traité sur l'Union européenne, autorisant les autorités désignées et Europol à avoir accès au VIS."

L'article 2 ("Définitions") comme suit:

"1. Aux fins de la présente décision, on entend par:

[...];

c) „infractions terroristes”: les infractions définies par le droit national qui correspondent ou sont équivalentes aux infractions visées aux articles 1^{er} à 4 de la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme;

d) „infractions pénales graves”: les formes de criminalité qui correspondent ou sont équivalentes à celles visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI;

[...]."

L'article 5 ("Conditions d'accès aux données du VIS par les autorités désignées des États membres") comme suit:

"1. L'accès au VIS en consultation est accordé aux autorités désignées, dans la limite de leurs pouvoirs et si les conditions suivantes sont réunies:

a) l'accès en consultation doit être nécessaire à la prévention, à la détection d'infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière;

b) un cas spécifique doit rendre l'accès en consultation nécessaire;

c) s'il existe des motifs raisonnables de considérer que la consultation des données du VIS contribuera de manière significative à la prévention ou à la détection des infractions en question, ou aux enquêtes en la matière.

[...]."

Code des visas

L' article 10 ("Règles générales applicables à l'introduction d'une demande") comme suit:

"1. Sans préjudice des dispositions des articles 13, 42, 43 et 45, les demandeurs se présentent en personne pour introduire leur demande.

[...].

3. Lorsqu'il introduit une demande, le demandeur:

[...];

c) présente une photographie conformément aux normes établies dans le règlement (CE) n o 1683/95 ou, là où le VIS est opérationnel, en application de l'article 48 du règlement VIS, conformément aux normes fixées à l'article 13 du présent règlement;

d) permet, s'il y a lieu, le relevé de ses empreintes digitales conformément à l'article 13;

[...]."

L'article 13 ("Éléments d'identification biométriques") comme suit:

"1. Les États membres recueillent les identifiants biométriques du demandeur, comprenant sa photographie et ses dix empreintes digitales, dans le respect des garanties prévues par la convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe, par la charte des droits fondamentaux de l'Union européenne et par la

convention des Nations unies relative aux droits de l'enfant.

2. Tout demandeur qui soumet sa première demande est tenu de se présenter en personne. Les identifiants biométriques ci-après du demandeur sont recueillis à cette occasion:

— une photographie, scannée ou prise au moment de la demande, et

— ses dix empreintes digitales, relevées à plat et numérisées.

3. Lorsque les empreintes digitales du demandeur recueillies dans le cadre d'une demande précédente ont été introduites pour la première fois dans le VIS moins de cinquante-neuf mois avant la date de la nouvelle demande, elles sont copiées lors de la demande ultérieure.

[...].

7. Les demandeurs ci-après sont dispensés de l'obligation de donner leurs empreintes digitales:

a) les enfants de moins de douze ans;

b) les personnes pour lesquelles il est physiquement impossible de recueillir les empreintes. S'il est possible de recueillir un nombre d'empreintes inférieur à dix, un recueil du nombre maximal d'empreintes est effectué. Toutefois, si l'impossibilité est temporaire, le demandeur est tenu de donner ses empreintes digitales lors de la demande suivante. Les autorités compétentes en vertu de l'article 4, paragraphes 1, 2 et 3, ont le droit de demander des précisions sur les motifs de l'impossibilité temporaire. Les États membres veillent à ce que des procédures appropriées garantissant la dignité du demandeur soient en place en cas de difficultés pour effectuer le recueil;

[...]."

Règlement d'Eurodac

Points 4 à 6, 8, 10, 15 et 22 du préambule comme suit:

"4. Il est nécessaire, aux fins de l'application du règlement (UE) no. 604/2013 [...], d'établir l'identité des demandeurs d'une protection internationale et des personnes interpellées à l'occasion du franchissement illégal d'une frontière extérieure de l'Union. Aux fins de l'application efficace du règlement (UE) n o 604/2013, et en particulier de son article 18, paragraphe 1, points b) et d), il est également souhaitable que tout État membre puisse vérifier si un ressortissant de pays tiers ou un apatride se trouvant illégalement sur son territoire a demandé une protection internationale dans un autre État membre.

5. Les empreintes digitales constituent un élément important aux fins de l'établissement de l'identité exacte de ces personnes. Il est nécessaire de créer un système de comparaison de leurs données dactyloscopiques.

6. À cette fin, il est nécessaire de créer un système dénommé "Eurodac", composé d'un système central, qui gérera une base de données dactyloscopiques centrale et informatisée, ainsi que des moyens électroniques de transmission entre les États membres et le système central, ci-après dénommé "infrastructure de communication".

8. En matière de lutte contre les infractions terroristes et les autres infractions pénales graves, il est essentiel que les autorités répressives disposent des informations les plus complètes et les plus récentes pour pouvoir exécuter leurs tâches. Les informations contenues dans Eurodac sont nécessaires aux fins de la prévention ou de la détection

d'infractions terroristes visées dans la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme ou d'autres infractions pénales graves visées dans la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, ou aux fins des enquêtes en la matière. Par conséquent, les autorités désignées des États membres et de l'Office européen de police (Europol) devraient avoir accès aux données d'Eurodac à des fins de comparaison sous réserve des conditions énoncées dans le présent règlement.

10. Dans sa communication au Conseil et au Parlement européen du 24 novembre 2005 sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, la Commission indiquait que les autorités chargées de la sécurité intérieure pourraient avoir accès à Eurodac dans des cas bien définis, lorsqu'il existe de bonnes raisons de croire que l'auteur d'une infraction terroriste ou d'une autre infraction pénale grave a demandé une protection internationale. Dans cette communication, la Commission précisait également qu'en vertu du principe de proportionnalité, Eurodac ne pouvait être interrogé à cette fin que si l'intérêt supérieur de la sécurité publique le commandait, c'est-à-dire si l'acte commis par le criminel ou le terroriste à identifier est si répréhensible qu'il justifie des recherches dans une base de données où sont enregistrées des personnes ayant un casier judiciaire vierge, et concluait que le seuil que devaient respecter les autorités chargées de la sécurité intérieure pour pouvoir interroger Eurodac devait donc toujours être sensiblement plus élevé que le seuil à respecter pour pouvoir interroger des bases de données criminelles.

15. Le présent règlement fixe également les conditions dans lesquelles les demandes de comparaison de données dactyloscopiques avec les données d'Eurodac aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière devraient être autorisées, ainsi que les garanties nécessaires pour assurer la protection du droit fondamental au respect de la vie privée des personnes dont les données à caractère personnel sont traitées dans Eurodac. La rigueur de ces conditions est le reflet du fait que la base de données Eurodac conserve les données dactyloscopiques de personnes qui sont présumées n'avoir commis aucune infraction terroriste ni aucune autre infraction pénale grave.

22. Il se peut que des ressortissants de pays tiers ou des apatrides qui ont demandé une protection internationale dans un État membre aient la possibilité de demander cette même protection dans un autre État membre pendant de nombreuses années encore. Par conséquent, la période maximale pendant laquelle les données dactyloscopiques devraient être conservées par le système central devrait être très longue. Étant donné que la plupart des ressortissants de pays tiers ou des apatrides qui sont installés dans l'Union depuis plusieurs années auront obtenu un statut de résident permanent, voire la nationalité d'un État membre à la fin de cette période, une période de dix ans devrait être considérée comme raisonnable pour la conservation de données dactyloscopiques."

L'article 2 ("Définitions") comme suit:

"1. Aux fins du présent règlement, on entend par:

a) "demandeur d'une protection internationale": un ressortissant de pays tiers ou un apatride qui a présenté une demande de protection internationale au sens de l'article 2, point h), de la directive 2011/95/UE, sur laquelle il n'a pas encore été statué définitivement;

[...].

i) "à des fins répressives": la prévention ou la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière;

j) "infractions terroristes": les infractions au titre du droit national qui correspondent ou sont équivalentes à celles visées aux articles 1^{er} à 4 de la décision-cadre 2002/475/JAI;

k) "infractions pénales graves": les formes de criminalité qui correspondent ou sont équivalentes à celles visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elles sont passibles, en droit national, d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans;

[...]."

L'article 9 ("Collecte, transmission et comparaison des empreintes digitales") comme suit:

"1. Chaque État membre relève sans tarder l'empreinte digitale de tous les doigts de chaque demandeur d'une protection internationale âgé de 14 ans au moins et la transmet au système central dès que possible et au plus tard 72 heures suivant l'introduction de la demande de protection internationale telle que définie à l'article 20, paragraphe 2, du règlement (UE) no 604/2013, accompagnée des données visées à l'article 11, points b) à g) du présent règlement.

[...]."

L'article 11 ("Enregistrement des données") comme suit:

"Seules sont enregistrées dans le système central les données suivantes:

a) données dactyloscopiques;

[...]."

L'article 12 ("Conservation des données") comme suit:

"1. Chaque ensemble de données visé à l'article 11 est conservé dans le système central pendant dix ans à compter de la date du relevé des empreintes.

2. Passé le délai visé au paragraphe 1, les données sont automatiquement effacées du système central par celui-ci."

L'article 13 ("Effacement anticipé des données") comme suit:

"1. Les données concernant une personne qui a acquis la nationalité d'un État membre, quel qu'il soit, avant l'expiration de la période visée à l'article 12, paragraphe 1, sont effacées du système central, conformément à l'article 27, paragraphe 4, dès que l'État membre d'origine apprend que la personne concernée a acquis ladite nationalité.

[...]."

L'article 14 ("Collecte et transmission des données dactyloscopiques") comme suit:

"1. Chaque État membre relève sans tarder l'empreinte digitale de tous les doigts de chaque ressortissant de pays tiers ou apatride, âgé de 14 ans au moins, qui, à l'occasion du franchissement irrégulier de sa frontière terrestre, maritime ou aérienne en provenance d'un pays tiers, a été interpellé par les autorités de contrôle compétentes et qui n'a pas été refoulé ou qui demeure physiquement sur le territoire des États membres et ne fait pas l'objet d'une mesure de confinement, de rétention ou de détention durant toute la période

comprise entre son interpellation et son éloignement sur le fondement de la décision de refoulement.

[...]."

L'article 16 ("Conservation des données") comme suit:

"1. Chaque ensemble de données relatives à un ressortissant de pays tiers ou à un apatride visé à l'article 14, paragraphe 1, est conservé dans le système central pendant dix-huit mois à compter de la date à laquelle ses empreintes digitales ont été relevées. Passé ce délai, le système central efface automatiquement ces données.

2. Les données relatives à un ressortissant de pays tiers ou à un apatride visé à l'article 14, paragraphe 1, sont effacées du système central conformément à l'article 28, paragraphe 3, dès que l'État membre d'origine a connaissance, avant l'expiration du délai de dix-huit mois visé au paragraphe 1 du présent article, de l'un des faits suivants:

- a) le ressortissant de pays tiers ou l'apatride s'est vu délivrer un document de séjour;
- b) le ressortissant de pays tiers ou l'apatride a quitté le territoire des États membres;
- c) le ressortissant de pays tiers ou l'apatride a acquis la nationalité d'un État membre, quel qu'il soit.

[...]."

L'article 20 ("Conditions d'accès à Eurodac par les autorités désignées") comme suit:

"1. Aux fins prévues à l'article 1^{er}, paragraphe 2, les autorités désignées ne peuvent présenter une demande électronique motivée de comparaison de données dactyloscopiques avec les données conservées dans le système central dans les limites de leurs compétences que si la comparaison dans les bases de données suivantes n'a pas permis de déterminer l'identité de la personne concernée:

- les bases de données dactyloscopiques nationales,
- les systèmes automatisés d'identification dactyloscopique de tous les autres États membres au titre de la décision 2008/615/JAI, si les comparaisons sont disponibles techniquement, à moins qu'il n'existe des motifs raisonnables de croire qu'une comparaison avec ces systèmes ne permettrait pas de déterminer l'identité de la personne concernée. Ces motifs raisonnables figurent dans la demande électronique motivée de comparaison avec les données d'Eurodac adressée par l'autorité désignée à l'autorité de vérification, et
- le système d'information sur les visas, pour autant que les conditions d'une telle comparaison prévues dans la décision 2008/633/JAI soient réunies;

et aux conditions cumulatives suivantes:

- a) la comparaison est nécessaire aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes en la matière, en ce sens qu'il existe un intérêt supérieur de sécurité publique qui rend la consultation de la base de données proportionnée;
- b) la comparaison est nécessaire dans un cas précis (c'est-à-dire des comparaisons systématiques ne peuvent être effectuées); et
- c) il existe des motifs raisonnables de penser que la comparaison contribuera de manière

significative à la prévention ou à la détection de l'une des infractions pénales en question ou aux enquêtes en la matière. De tels motifs raisonnables existent en particulier lorsqu'il existe des motifs de soupçonner que le suspect, l'auteur ou la victime d'une infraction terroriste ou d'une autre infraction pénale grave relève d'une catégorie couverte par le présent règlement. [...]."