Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2017–2018

34 867 EU-voorstellen inzake tweede pakket interoperabiliteit COM(2017)793 en 794[1]

A

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 23 april 2018

De leden van de vaste commissies voor Immigratie en Asiel / JBZ-Raad[2] en voor Justitie en Veiligheid[3] hebben kennisgenomen van de twee verordeningsvoorstellen van de Europese Commissie inzake interoperabiliteit tussen EU-informatiesystemen op het terrein van migratie, grensbeheer en veiligheid[4] en het bijbehorende BNC-fiche van de regering.[5] Naar aanleiding hiervan is op 13 maart 2018 een brief gestuurd aan de Minister van Justitie en Veiligheid.

De Minister heeft op 23 april 2018 gereageerd.

De commissies brengen bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier voor dit verslag,
Van Dooren

---

[1] Zie dossier E180007 op www.europapoort.nl

[2] Samenstelling **Immigratie en Asiel/JBZ-Raad**:
Engels (D66), Nagel (50plus), Van Bijsterveld (CDA), Duthler (VVD), Ten Hoeve (OSF), Schaap (VVD), Strik (GL) (*vice-voorzitter*), Knip (VVD, Faber-van de Klashorst (PVV), Schouwenaar (VVD), Gerkens (SP), Bredenoord (D66), Dercksen (PVV) *(voorzitter),* D.J.H. van Dijk (SGP), Van Hattem (PVV), Knapen (CDA), Nooren (PvdA), Oomen-Ruijten (CDA), Rombouts (CDA), Stienen (D66), Teunissen (PvdD), Wezel (SP), Bikker (CU), Overbeek (SP), Van Zandbrink (PvdA),), Fiers PvdA)

[3] Samenstelling **Justitie en Veiligheid**:
Engels (D66), Ruers (SP), Van Bijsterveld (CDA) (*vice-voorzitter*), Duthler (VVD) *(voorzitter),* Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Knip (VVD), Backer (D66), Schouwenaar (VVD), Van Strien (PVV), Kok (PVV), Gerkens (SP), Vlietstra (PvdA), Lokin-Sassen (CDA), Bredenoord (D66), Dercksen (PVV), D.J.H. van Dijk (SGP), Van Rij (CDA), Rombouts (CDA), Van de Ven (VVD), Wezel (SP), Bikker (CU), Baay-Timmerman (50PLUS) Van Zandbrink (PvdA), Aardema (PVV), Fiers (PvdA)

[4] COM(2017)793 en COM(2017)794.

[5] *Kamerstukken II* 2017/18, 22 112, nr 2479.

kst-34867-A
ISSN 0921 - 7371
's-Gravenhage 2018

BRIEF VAN DE VOORZITTERS VAN DE VASTE COMMISSIES VOOR IMMIGRATIE EN ASIEL/JBZ-RAAD EN VOOR JUSTITIE EN VEILIGHEID

Aan de Minister van Justitie en Veiligheid

Den Haag, 13 maart 2018

De leden van de vaste commissies voor Immigratie en Asiel / JBZ-Raad en voor Justitie en Veiligheid hebben kennisgenomen van de twee verordeningsvoorstellen van de Europese Commissie inzake interoperabiliteit tussen EU-informatiesystemen op het terrein van migratie, grensbeheer en veiligheid[6] en het bijbehorende BNC-fiche van de regering.[7] De leden van de **GroenLinks**-fractie hebben naar aanleiding hiervan de volgende vragen en opmerkingen.

Nut en noodzaak

Met dit wetgevingspakket worden de persoonsgegevens van verschillende Europese databanken aan elkaar gekoppeld. Kunt u aangeven waarom dit voorstel noodzakelijk zou zijn voor de grenscontrole en een verhoogde interne veiligheid? Ziet u het risico dat de koppeling ook leidt tot meer complexiteit, wat de handhaving juist ook verder kan bemoeilijken? Het gaat hier immers om databestanden met verschillende typen data en verschillende doeleinden.

In het BNC-fiche wordt gesteld dat de regering de proportionaliteit van de voorstellen positief beoordeeld.[8] Kunt u deze appreciatie nader onderbouwen, mede in het licht van de reserves die de regering op onderdelen heeft geuit?

Hoe verhouden de voorstellen voor het opvragen en vergelijken van biometrische gegevens zich tot de huidige uitwisselingsmogelijkheden voor rechtshandhavingsdoeleinden op basis van het Prüm besluit?[9] Welke aanvullende mogelijkheden worden hiermee geboden?

Bescherming van persoonsgegevens

De Europese Commissie heeft een impact assessment gedaan, maar in hoeverre vormde een privacy impact assessment hiervan effectief een onderdeel? Op welke wijze is de impact op de privacy onderzocht? Bent u bereid de privacy impact te betrekken in de nationale quickscan impactanalyse? Welke precieze onderzoeksvragen vormen de basis van deze analyse?

Op welke wijze zijn de doeleinden voor inzage en gebruik van de data gelimiteerd en gelegitimeerd? In hoeverre is dit in overeenstemming met het doelbindingsprincipe van de Algemene Verordening Gegevensbescherming (AVG)?[10] In hoeverre vergroten de voorstellen het risico van het zogeheten *function creep*? Kunt u meer in het algemeen toelichten in hoeverre de voorstellen in overeenstemming zijn met de AVG en met richtlijn 2016/680? Wanneer is de verordening en wanneer is de richtlijn van toepassing? Is het voorstelbaar dat beide tegelijk van toepassing zijn op een uitwisseling en hoe werkt dat dan in de praktijk?

---

[6] COM(2017)793 en COM(2017)794.
[7] *Kamerstukken II* 2017/18, 22 112, nr 2479.
[8] *Kamerstukken II* 2017/18, 22 112, nr 2479, p. 10.
[9] Besluit 2008/615/JBZ.
[10] Verordening (EU) 2016/679.

Toegang tot de informatiesystemen

Kunt u aangeven welke autoriteiten er precies toegang hebben tot deze databanken? En ontvangen deze autoriteiten hierdoor meer informatie dan voorheen? Zo ja, in hoeverre is de noodzaak hiervoor aangetoond? Welke problemen ondervinden de autoriteiten momenteel doordat ze geen toegang tot de databanken hebben?

Recht van inzage, rectificatie en wissing

Welke mogelijkheden hebben burgers om te controleren welke informatie er over hen beschikbaar is en hoe deze wordt gebruikt? Acht u het proportioneel dat de gegevens van individuele burgers in complexe systemen worden opgeslagen zonder dat zij inzicht hebben in de gegevens en het gebruik ervan, en dus evenmin een mogelijkheid hebben om de data te controleren op juistheid, te corrigeren of te verzoeken om vernietiging? In welke situaties zou er volgens u sprake moeten zijn van een notificatieplicht? En hoe is de kwaliteit en juistheid van de gegevens te waarborgen? Welke garanties zijn er voor de bescherming van de databanken tegen hacken, aanvallen of manipulaties van buitenaf?

Bewaartermijnen

De betreffende databanken kennen verschillende maximale bewaarperiodes. Is het zo dat door de uitwisseling van gegevens de informatie uit een databank langer dan de maximale duur kan worden bewaard in een andere databank waar langere termijnen gelden, op zijn minst de informatie dat er data waren opgeslagen in die eerste databank? En zo ja, hoe verhoudt zich dat tot de privacyverordening en richtlijn?

Non-discriminatie

Kunt u uiteenzetten wat de verschillen zullen zijn in rechtspositie voor EU-burgers, burgers uit derde landen met een EU-nationaliteit en burgers uit derde landen en hoe zijn deze verschillen gerechtvaardigd? Beschikken al deze groepen bijvoorbeeld over dezelfde mate van rechtsbescherming en toegang tot het Europees Hof van Justitie indien hun rechten door eventueel misbruik van het datasysteem worden geschonden? In hoeverre zijn deze verschillen in overeenstemming met het verbod op discriminatie, mede gelet op het HvJ arrest Huber tegen Duitsland[11] waar het Hof duidelijk maakte dat onderscheid naar nationaliteit niet gerechtvaardigd is als de maatregel tot doel heeft de criminaliteit te bestrijden. Worden al deze groepen niet op gelijke wijze beschermd door artikel 7 en 8 Handvest, de AVG en de fundamentele beginselen van de Unie?

Kunt u ingaan op het risico van stigmatisering en etnische profilering, nu de autoriteiten ook de mogelijkheid wordt gegeven om derdelanders niet alleen aan de grens maar ook op het EU grondgebied te controleren op hun identiteit?

Overig

Tot slot verwijzen de leden van de GroenLinks-fractie naar een Raadsdocument[12] dat door het Bulgaars Voorzitterschap is opgesteld ten behoeve van een oriënterend debat in de JBZ-Raad van 8-9 maart jl. In dit

[11] HvJ EG 16 december 2008, C-524/06, ECLI:EU:C:2008:724 (*Huber / Bundesrepublik Deutschland*).
[12] Raadpleegbaar via het register van de Raad met documentnummer 6396/18.

document worden een aantal vragen gesteld aan de lidstaten. Bent u bereid om de antwoorden op deze vragen aan de Kamer te zenden?

De leden van de vaste commissies voor Immigratie en Asiel / JBZ-Raad en voor Justitie en Veiligheid zien uw antwoord met belangstelling tegemoet en ontvangen deze graag uiterlijk binnen vier weken na dagtekening van deze brief.

Voorzitter van de vaste commissie voor Immigratie en Asiel / JBZ-Raad,
R.G.J. Dercksen

Voorzitter van de vaste commissie voor Justitie en Veiligheid,
A.W. Duthler

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 23 april 2018

Hierbij zend ik u mede namens de Staatssecretaris van Justitie en Veiligheid de antwoorden op de vragen van de GroenLinksfractie over de verordeningsvoorstellen Interoperabiliteit tussen de centrale EU-informatiesystemen informatiesystemen in het Justitie en Binnenlandse Zaken domein (162633u).

De Minister van Justitie en Veiligheid,
F.B.J. Grappperhaus

Antwoorden van de Minister van Justitie en Veiligheid over de over de verordeningsvoorstellen Interoperabiliteit tussen de centrale EU-informatiesystemen.

Met deze brief beantwoord ik uw vragen met betrekking tot de verordeningsvoorstellen Interoperabiliteit tussen de centrale EU-informatiesystemen in het Justitie en Binnenlandse Zaken domein. Naar aanleiding van een AO behandelvoorbehoud met de Tweede Kamer heb ik onlangs aan de Tweede Kamer een uitgebreide toelichtende brief over de interoperabiliteitsvoorstellen gestuurd tezamen met het verslag JBZ-Raad 8 en 9 maart. Waar dat opportuun is, verwijs ik voor de beantwoording van uw vragen naar die toelichtende brief die als bijlage is bijgevoegd waarin de belangrijkste aandachtspunten ten aanzien van de interoperabiliteitsvoorstellen zijn uitgewerkt, zoals de meerwaarde van interoperabiliteit, gegevensbescherming en gevolgen voor andere grondrechten. Met de Tweede Kamer is tijdens het algemeen overleg over het behandelvoorbehoud op 22 februari jl. afgesproken haar periodiek te informeren over de voortgang van de onderhandelingen. Ik zal deze informatie eveneens aan uw Kamer toezenden.

Nut en noodzaak

Vraag
Met dit wetgevingspakket worden de persoonsgegevens van verschillende Europese databanken aan elkaar gekoppeld. Kunt u aangeven waarom dit voorstel noodzakelijk zou zijn voor de grenscontrole en een verhoogde interne veiligheid?

Antwoord
Graag verwijs ik u naar de brief in de bijlage waar ik onder de kop «voordelen interoperabiliteit» (pagina 3) en «meerwaarde hit/no-hit-systeem» (pagina 5) uiteengezet waar ik de toegevoegde waarde zie van deze voorstellen en heb daarbij, tevens een drietal voorbeelden gegeven.

Vraag
Ziet u het risico dat de koppeling ook leidt tot meer complexiteit, wat de handhaving juist ook verder kan bemoeilijken? Het gaat hier immers om databestanden met verschillende typen data en verschillende doeleinden.

Antwoord
Het is van belang dat voldoende aandacht wordt besteed aan de kwaliteit van gegevens waarvan de interoperabiliteitscomponenten gebruikmaken maken en dat daarop toezicht wordt uitgeoefend. Een slechte datakwaliteit kan met de koppeling van gegevens immers grote gevolgen hebben voor het handelen ten aanzien van bonafide personen. Ik ben dan ook verheugd dat de Europese Commissie in de voorstellen de nodige extra maatregelen voorziet op dit terrein. Zo is er aandacht voor training van eindgebruikers, worden via implementatieregels nog afspraken gemaakt over de inrichting van werkprocessen, wordt gestandaardiseerd op de «taal» van de verschillende systemen door middel van het «universal message format», worden kwaliteitsindicatoren vastgesteld en wordt voorzien in «Automated Data Quality Control Mechanisms» waarmee patronen kunnen worden onderkend en fouten worden gesignaleerd. Verder zullen eu-LISA en de Commissie elk jaar aan de lidstaten rapporteren over de datakwaliteit en met aanbevelingen voor verbetering komen. Verder bevatten de voorstellen belangrijke waarborgen op basis waarvan toezicht kan worden gehouden, zoals logging- en monitoringsvereisten en beveiligingsvoorschriften. Deze waarborgen zijn essentieel voor de toezichtshandelingen. Ook op nationaal niveau zal er aandacht zijn voor het trainen en opleiden van eindgebruikers, hetgeen ten goede

zal komen aan de kwaliteit van de informatie. Technische oplossingen moeten ondersteunend zijn en om de informatiekwaliteit te waarborgen moet er in belangrijke mate aandacht zijn voor de menselijke factor in gegevensverwerking. Daarnaast wordt door interoperabiliteit inzicht gekregen in de mate waarin personen gebruik maken van meerdere identiteiten. Dit leidt tot het beter detecteren van identiteitsfraude, verschrijvingen en fouten in de registratie waardoor de EU informatiehuishouding beter op orde komt. De verificatie van de verbanden tussen identiteiten, uitgedrukt in links naar data uit de verschillende systemen, kan potentieel complex zijn maar beoogt sneller, meer relevante data bij elkaar te brengen waardoor het proces tot een accurate identiteitsvaststelling sneller en effectiever verloopt, wat een gunstig effect heeft op de gehele complexiteit van het identificatieproces.
Het is inderdaad zo dat de voorstellen betrekking hebben op verschillende systemen die verschillende typen gegevens bevatten met verschillende doeleinden. Zoals ook uiteengezet in de brief die is toegevoegd in de bijlage bepalen de voorstellen dat deze gegevens van verschillende categorieën betrokkenen, de «data subjects», strikt van elkaar gescheiden moeten worden. De «Common Identity Repository» houdt rekening met de noodzaak tot het compartimenteren van de gegevens op grond van het doel van het systeem waarvoor ze zijn verstrekt. Dit komt niet alleen de gegevensbescherming maar ook het beheer van de gegevens ten goede, waarbij de maatregelen voorzien in de wettelijke basis van de individuele systemen bepalend is. Alleen het beheer van links tussen identiteitsgegevens en de zogenoemde biometrische templates in de gemeenschappelijke «Biometric Matching Service» zijn aanvullende gegevens ten opzichte van de afzonderlijke systemen en de daartoe ondersteunende «Common Identity Repository». Het gaat om gegevens die bijdragen aan het sneller doorgronden van de complexiteit van de beschikbare gegevens en om vast te stellen welke gegevens van waarde zijn en welke juist niet. Dat laat onverlet dat het proces ter verificatie van de gegevens die de interoperabiliteitvoorstellen voorschrijven doelmatig, met strikte waarborgen omgeven en met beperkt lastendruk gerealiseerd moet worden en dat de eindgebruiker aan de grens en op straat eenduidige informatie krijgt om doeltreffend op te treden.

Vraag
In het BNC-fiche wordt gesteld dat de regering de proportionaliteit van de voorstellen positief beoordeeld. Kunt u deze appreciatie nader onderbouwen, mede in het licht van de reserves die de regering op onderdelen heeft geuit?

Antwoord
Het kabinet is positief over de maatregelen in de voorstellen omdat deze geschikt en noodzakelijk zijn om de structurele tekortkomingen van de huidige EU informatiemanagementarchitectuur op te lossen en daarmee bijdragen aan het beheer van de buitengrens van het Schengengebied en de interne veiligheid van de EU. Een verordening is hiervoor voorts het geëigende instrument. Dat laat onverlet dat het kabinet voor de uitvoering kritisch blijft kijken naar de lastendruk bij autoriteiten in het geval mogelijke meervoudige biografische identiteiten voor het individu in de systemen worden aangetroffen. Lidstaten zullen handmatige controles moeten gaan uitvoeren in het geval dat iemand naar verwachting gebruik maakt van meerdere identiteiten. Deze controles zijn onderdeel van een systeem overstijgend verificatieproces van data voor een goede vaststelling van identiteiten. Het betreft een nieuw proces dat toegevoegde waarde biedt zoals in voorgaande vraag uiteengezet, maar waarvan de lastendruk voor taakorganisaties evenals de noodzakelijke waarborgen nauwlettend zullen worden gemonitord. Deze punten zullen dan ook worden meegenomen in de nationale QuickScan analyse om

meer inzicht in te verkrijgen. Bovendien wordt het van belang geacht dat de interoperabiliteitsvoorstellen niet de huidige EU en nationale informatiearchitectuur onder druk zetten.

Volgens de voorstellen zou ook het ECRIS-TCN gebruikmaken van de verschillende componenten van interoperabiliteit. In het BNC fiche heeft het kabinet aangegeven op basis van de gepresenteerde voorstellen niet overtuigd te zijn van de noodzaak en proportionaliteit van het betrekken van justitiële gegevens uit ECRIS-TCN. Dit zal nadere uitleg en uitwerking vergen.

Vraag
Hoe verhouden de voorstellen voor het opvragen en vergelijken van biometrische gegevens zich tot de huidige uitwisselingsmogelijkheden voor rechtshandhavingsdoeleinden op basis van het Prüm besluit? Welke aanvullende mogelijkheden worden hiermee geboden?

Antwoord
Ook hier kan ik verwijzen naar de brief in de bijlage. Het tweede voorbeeld op pagina 3 van de brief illustreert hoe de voorstellen zich verhouden tot de Prüm besluiten. Dit tweede voorbeeld betreft de situatie waarbij in geval van zware criminaliteit of terrorisme uit een opsporingsonderzoek blijkt dat een verdachte meerdere aliassen gebruikt. Momenteel moet de politie om met dit doel de identiteit van een persoon vast te stellen eerst nagaan of biometrische gegevens bekend zijn in nationale registers en het decentrale Prüm-systeem raadplegen aan de hand van een vingerafdruk. Als deze procedure niets oplevert, kan toegang worden verzocht tot de centrale EU migratie gerelateerde informatiesystemen. Bovendien is op dat moment niet bekend welke systemen informatie over deze persoon bevatten. Door interoperabiliteit kan parallel aan de raadpleging van het decentrale Prüm-systeem op hit/no-hit-basis, op een efficiënte wijze worden gezocht naar relevante biometrische gegevens in de «Common Identity Repository» en de daartoe ondersteunende «Biometric Matching Service». Hierna kan vervolgens, conform de bestaande wettelijke voorwaarden, met een omkleed verzoek bij een centraal contactpunt om toegang worden verzocht tot informatie over de desbetreffende persoon in het individuele informatiesysteem dat de hit verschaft. Doordat een hit al aangetoond heeft welke informatiesystemen gegevens bevatten, worden onnodige verzoeken om toegang te verkrijgen tot die informatie voorkomen. De hit wordt enkel getoond aan de gebruiker die ook daadwerkelijk deze toegang kan verkrijgen, conform de daarvoor geldende procedures en toegangsrechten. Bovendien bieden de interoperabiliteitsvoorstellen de mogelijkheid om te zoeken met behulp van gelaatscans (via de «Biometric Matching Service»), hetgeen niet mogelijk is op basis van het Prüm besluit. Het Prüm besluit biedt namelijk qua biometrische gegevens enkel de mogelijkheid om DNA en dactyloscopische gegevens uit te wisselen.

Bescherming van persoonsgegevens

Vraag
De Europese Commissie heeft een impact assessment gedaan, maar in hoeverre vormde een privacy impact assessment hiervan effectief een onderdeel? Op welke wijze is de impact op de privacy onderzocht?

Antwoord
Het impact assessment van de Commissie heeft gekeken naar de impact van de wetgeving voor fundamentele rechten, en daarbij specifiek aandacht besteed aan gegevensbescherming. Hierbij is per component van interoperabiliteit gekeken naar de impact op gegevensbescherming.

De haalbaarheid van interoperabiliteit wordt aangereikt aan de hand van drie beleidsopties, zoals ook toegelicht in het BNC-fiche. Bij elke optie is ook gekeken naar de impact op gegevensbescherming. Bij de gekozen optie wordt in het impact assessment geconcludeerd dat de impact op het recht op privacy is beperkt tot het strikt noodzakelijke. Ten aanzien van de gevolgen van interoperabiliteit voor de fundamentele rechten en het recht op bescherming van persoonsgegevens benadrukt het impact assessment dat de interoperabiliteits-componenten vanwege het aanvullende karakter niets veranderen aan het evenwicht dat reeds door elk van de bestaande centrale systemen is bereikt met betrekking tot hun effect op fundamentele rechten. De voorgestelde interoperabiliteitsmaatregelen moeten worden beschouwd als complementaire componenten voor de afzonderlijke centrale systemen waarvoor een strikte doelbinding geldt.

Wat betreft de gegevensbescherming wens ik te benadrukken dat de Europese Gegevensbeschermingsautoriteit – European Data Protection Supervisor (EDPS) – binnenkort een tweede opinie over de voorstellen zal verstrekken. Daarnaast zal het EU Grondrechtenagentschap – Fundamental Rights Agency (FRA) – binnenkort een opinie verstrekken. Ook deze opinies zal ik betrekken in het verdere onderhandelproces en bij de positie die Nederland inneemt in het bijzonder inzake de noodzakelijke waarborgen voor gegevensbescherming.
Daarbij moet worden vermeld dat beide instanties in de discussies over de interoperabiliteitconcepten als waarnemer door de Europese Commissie betrokken zijn en voorafgaand aan de publicatie van de voorstellen opinies over interoperabiliteit en de door de Europese Commissie beoogde concepten hebben uitgevaardigd.

Vraag
Bent u bereid de privacy impact te betrekken in de nationale quickscan impactanalyse? Welke precieze onderzoeksvragen vormen de basis van deze analyse?

Antwoord
Ja, bij de nationale QuickScan zal privacy impact worden betrokken. De precieze onderzoeksvragen zullen nog worden geformuleerd.

Vraag
Op welke wijze zijn de doeleinden voor inzage en gebruik van de data gelimiteerd en gelegitimeerd? In hoeverre is dit in overeenstemming met het doelbindingsprincipe van de Algemene Verordening Gegevensbescherming (AVG)? In hoeverre vergroten de voorstellen het risico van het zogeheten «function creep»? Kunt u meer in het algemeen toelichten in hoeverre de voorstellen in overeenstemming zijn met de AVG en met richtlijn 2016/680? Wanneer is de verordening en wanneer is de richtlijn van toepassing? Is het voorstelbaar dat beide tegelijk van toepassing zijn op een uitwisseling en hoe werkt dat dan in de praktijk?

Antwoord
Ten aanzien van uw vragen over gegevensbescherming merk ik op dat zoals in het BNC-fiche aangegeven, ik het belang van interoperabiliteit van de desbetreffende EU-informatiesystemen onderschrijf. Maar tegelijkertijd is het Nederlands beleid en is het onze plicht om de grondrechten van het individu te beschermen. Ik zal dan ook onverkort aandacht blijven vragen voor de bescherming van deze rechten. In de eerder genoemde brief die als bijlage is meegezonden, ga ik onder de kop doelbinding (pagina 4) en gegevensbescherming (pagina 6) hier uitgebreid op in.
Aanvullend kan ik u melden dat het concept van interoperabiliteit is ontworpen conform de principes van «privacy by design» (gegevensbescherming door ontwerp) en «privacy by default» (gegevensbescherming

door standaardinstellingen), waar ook de European Data Protection Supervisor herhaaldelijk aandacht voor heeft gevraagd. Gegevensbescherming wordt meegenomen in het ontwerp en de architectuur van de bestaande en nieuwe informatiesystemen en de interoperabiliteitscomponenten, waarbij rekening is gehouden met beginselen zoals doelbinding, minimale gegevensverwerking, opslagbeperking en het kunnen garanderen van een passende beveiliging van persoonlijke gegevens.

Voor wat betreft uw vraag over op welke wijze de doeleinden voor inzage en gebruik van de data gelimiteerd en gelegitimeerd zijn, merk ik op dat de doelen van de individuele informatiesystemen en daarin vergaarde informatie niet wijzigen met deze voorstellen. Wel worden secundaire aanvullende doelen voorgesteld zoals uiteengezet in de bijgesloten bijlage onder de kop doelbinding (pagina 4) ter fine van een accurate identiteitsvaststelling. De legitimatie daarvoor – zoals uiteengezet in de bijlage – ligt vervat in de noodzaak om voor ieder hoofddoel, zij het voor migratiebeheer, grensbeheer, opsporing en vervolging of handhaving, primair vast te stellen wat de identiteit van een persoon is, die onderhevig is aan handelingen verbonden aan één of meerdere hoofddoelen, en deze zo accuraat mogelijk vast te stellen. Dit draagt bij aan een goede dienstverlening aan bonafide derdelanders, een doeltreffende aanpak van identiteitsfraude en het versterken van de rechtsbescherming van het individu.
Voor wat betreft uw vraag wanneer de verordening en wanneer de richtlijn van toepassing is, bepalen de voorstellen dat in principe de Algemene Verordening Gegevensbescherming (AVG) van toepassing is, tenzij gegevens worden verwerkt door een aangewezen autoriteit of centrale toegangspunt in het kader van het voorkomen, opsporen of onderzoeken van terroristische misdrijven of andere ernstige criminaliteit. Nationale toezichthouders die zijn ingesteld conform de AVG zullen de rechtmatigheid van de gegevensverwerking door lidstaten monitoren. Voor wat betreft gegevensverwerking door de EU organen en agentschappen, zal het monitoren gebeuren door de European Data Protection Supervisor, ingesteld conform Verordening 45/2001 en de Europol verordening 2016/794.
Voor wat betreft het toepassingsbereik sluiten de AVG en de richtlijn elkaar wederzijds uit: waar de richtlijn geldt, is de verordening niet van toepassing en andersom. Materieel is er sprake van een zekere mate van overlap tussen de richtlijn en de verordening voor wat betreft de verplichtingen van de verwerkingsverantwoordelijke. Dat laat onverlet dat ook in dit kader training van eindgebruikers van de systemen en informatie van belang is zodat de juiste maatregelen worden getroffen en uitgevoerd zoals voorgeschreven door de respectievelijke EU wetgeving en nationale implementatiewetgeving.

Toegang tot de informatiesystemen

Vraag
Kunt u aangeven welke autoriteiten er precies toegang hebben tot deze databanken? En ontvangen deze autoriteiten hierdoor meer informatie dan voorheen? Zo ja, in hoeverre is de noodzaak hiervoor aangetoond? Welke problemen ondervinden de autoriteiten momenteel doordat ze geen toegang tot de databanken hebben?

Antwoord
In de brief die als bijlage is meegestuurd wordt uiteengezet welke autoriteiten toegang krijgen tot de databanken. Ook wordt hier aangegeven of deze autoriteiten meer informatie krijgen dan voorheen. Wat betreft het tweede deel van uw vraag verwijs ik graag naar mijn antwoorden onder de voordelen van interoperabiliteit (pagina 3) van dit

schrijven. Voor het eerste element, de verificatie van een identiteit en het vaststellen van de leidende identiteit van de persoon, worden de autoriteiten die toegang kunnen verkrijgen tot de gegevens in de informatiesystemen, beschreven in de voorstellen. Het betreft de autoriteiten bevoegd onder wetgevende instrumenten van de betreffende informatiesystemen. In het geval van het tweede element, de bestrijding van zware criminaliteit en terrorisme, hebben rechtshandhavingsautoriteiten al toegang tot identiteitsinformatie uit niet-rechtshandhavingsinformatiesystemen. Zoals uiteengezet in de brief in de bijlage, worden deze toegangsrechten niet uitgebreid (er kan nu immers conform de daarvoor geldende voorwaarden ook al toegang gevraagd worden tot deze niet-rechtshandhavingsinformatiesystemen). De verandering is gelegen in het beschikbaar stellen van de hit/no-hit functionaliteit. De noodzaak daarvoor vloeit voort uit het feit dat door het beschikbaar stellen van de beperkte informatie dat er gegevens beschikbaar zijn in een informatiesysteem, op een snellere en efficiëntere wijze informatie kan worden opgevraagd over een persoon. Als van te voren bekend is in welke informatiesystemen relevante informatie aanwezig is, hoeven alleen die specifieke systemen bevraagd te worden, waarmee het noodzakelijkheidsprincipe bij het opvragen van informatie beter wordt ingevuld. Voor wat betreft het derde element, verschaffen de voorstellen de grondslag om voor het vaststellen van een identiteit, op nationaal niveau, omkleed met de nodige wettelijke waarborgen, politieautoriteiten direct toegang te verlenen tot de identiteitsdata opgenomen in de «Common Identity Repository». Het invullen van deze grondslag (of en op welke wijze) dient nationaal te worden bepaald.
Wat betreft het laatste deel van uw vraag over de problemen die autoriteiten ondervinden, kan ik u melden dat deze onder meer zijn de afwezigheid van identiteitspapieren bij derdelanders wanneer ze worden aangetroffen, vervalsingen van identiteitsdocumenten, het gebruik van aliassen, inzet van zogenoemde «look-a-likes», verschrijvingen bij de registratie van identiteitsgegevens, verschillen in de invoer van identiteitsgegevens tussen lidstaten.

Recht van inzage, rectificatie en wissing

Vraag
Welke mogelijkheden hebben burgers om te controleren welke informatie er over hen beschikbaar is en hoe deze wordt gebruikt? Acht u het proportioneel dat de gegevens van individuele burgers in complexe systemen worden opgeslagen zonder dat zij inzicht hebben in de gegevens en het gebruik ervan, en dus evenmin een mogelijkheid hebben om de data te controleren op juistheid, te corrigeren of te verzoeken om vernietiging? In welke situaties zou er volgens u sprake moeten zijn van een notificatieplicht? En hoe is de kwaliteit en juistheid van de gegevens te waarborgen? Welke garanties zijn er voor de bescherming van de databanken tegen hacken, aanvallen of manipulaties van buitenaf?

Antwoord
In de eerder aangehaalde brief die als bijlage is toegevoegd wordt op het onderdeel recht van inzage, rectificatie en verwijdering eveneens ingegaan Dat is naar aanleiding van een schrijven van de Commissie Meijer (pagina 9) waarop ik op verzoek van de Tweede Kamer een reactie heb gegeven. Gegevens van burgers worden inderdaad opgeslagen, maar de voorstellen voorzien wel, onder bepaalde voorwaarden en rekening houdende met de uitzonderingen zoals ook in de AVG en dataprotectierichtlijn opgenomen, in een recht op inzage, evenals rectificatie en verwijdering. Voor wat betreft uw vraag over de kwaliteit en juistheid van de gegevens evenals over de bescherming van de databanken tegen hacken, aanvullen of manipulaties van buitenaf, is het van belang dat de

gegevens fysiek op verschillende servers worden opgeslagen. De lidstaten en eu-LISA moeten veiligheidsplannen opstellen ter implementatie van de veiligheidsverplichtingen en met elkaar samenwerken ten behoeve van het garanderen van deze veiligheid. Deze veiligheidsverplichtingen beogen onder andere om de data fysiek te beschermen, ongeautoriseerde toegang en ongeautoriseerde gegevensverwerking te voorkomen. Eu-LISA moet bovendien gebruik maken van de laatste technologische ontwikkelingen om de data-integriteit te kunnen garanderen, in het kader van het ontwikkelen, ontwerpen en het beheer van de interoperabiliteits-componenten. In het geval van een veiligheidsincident, bestaat de verplichting voor lidstaten om de Commissie, eu-LISA en de European Data Protection Supervisor hiervan te notificeren Daarnaast is er de verplichting om dit te melden aan de toezichthoudende autoriteit, conform de AVG ofwel de Richtlijn.

Bewaartermijnen

Vraag
De betreffende databanken kennen verschillende maximale bewaarperiodes. Is het zo dat door de uitwisseling van gegevens de informatie uit een databank langer dan de maximale duur kan worden bewaard in een andere databank waar langere termijnen gelden, op zijn minst de informatie dat er data waren opgeslagen in die eerste databank? En zo ja, hoe verhoudt zich dat tot de privacyverordening en -richtlijn?

Antwoord
Ingevolge de huidige voorstellen wordt een individueel bestand in de «Common Identity Repository» bewaard zolang de daarbij behorende gegevens bewaard zijn in ten minste één van de onderliggende informatiesystemen. In dit verband heb ik in de onderhandelingen benadrukt dat de bewaartermijnen hiermee niet mogen worden opgerekt, bijvoorbeeld in het geval dat een individueel bestand bestaat uit gegevens van twee informatiesystemen met verschillende bewaartermijnen.

Non-discriminatie

Vraag
Kunt u uiteenzetten wat de verschillen zullen zijn in rechtspositie voor EU-burgers, burgers uit derde landen met een EU-nationaliteit en burgers uit derde landen en hoe zijn deze verschillen gerechtvaardigd? Beschikken al deze groepen bijvoorbeeld over dezelfde mate van rechtsbescherming en toegang tot het Europees Hof van Justitie indien hun rechten door eventueel misbruik van het datasysteem worden geschonden? In hoeverre zijn deze verschillen in overeenstemming met het verbod op discriminatie, mede gelet op het HvJ arrest Huber tegen Duitsland waar het Hof duidelijk maakte dat onderscheid naar nationaliteit niet gerechtvaardigd is als de maatregel tot doel heeft de criminaliteit te bestrijden. Worden al deze groepen niet op gelijke wijze beschermd door artikel 7 en 8 Handvest, de AVG en de fundamentele beginselen van de Unie?

Antwoord
Het algemene doel van de voorstellen betreft de bescherming van de buitengrens en bescherming van de veiligheid van de EU. Hierop zijn de verschillende doelstellingen van de voorstellen gebaseerd, zoals uiteengezet in het BNC-fiche. De gemeenschappelijke deler van de verschillende informatiesystemen is dat deze gegevens bevatten omtrent derdelanders. Alleen het SIS bevat ook data over EU burgers, maar deze data worden op grond van de voorstellen niet opgenomen in de «Common Identity Repository». Indien data in de «Common Identity Repository» een relatie hebben met data in het SIS over een persoon, dan

zal de eigenaar van de SIS signalering direct deze data analyseren met behulp van biometrische data. In de eerder aangehaalde brief die als bijlage is toegevoegd, beantwoord ik uw vragen verder op pagina's 9 en 10.

Vraag
Kunt u ingaan op het risico van stigmatisering en etnische profilering, nu de autoriteiten ook de mogelijkheid wordt gegeven om derdelanders niet alleen aan de grens maar ook op het EU grondgebied te controleren op hun identiteit?

Antwoord
Wat betreft het risico van stigmatisering en etnische profilering het volgende. Identiteitsvaststelling vindt op dit moment in Nederland plaats in het kader van de Vreemdelingenwet voor visumverlening, het asielproces, reguliere immigratie en in het kader van grensbewaking en toezicht. De mogelijkheid de «Common Identity Repository» te raadplegen zal hier geen verandering in aanbrengen. In het geval de politie naar de identiteit wil vragen, is daarvoor een aanleiding nodig: er moet steeds een geldige reden zijn, gebaseerd op een taak, zoals de politietaak of die van een toezichthouder. Het vorderen van inzage in een identiteitsbewijs dient bovendien niet alleen te geschieden in het kader van de uitoefening van de (politie)taak, maar inzage moet ook redelijkerwijs noodzakelijk zijn voor de vervulling van die taak. De aanleiding kan niet gelegen zijn in de beschikbaarheid van data. Kortom, indien een persoon zich niet kan identificeren mag de politieambtenaar alleen op grond van een geldige reden de «Common Identity Repository» raadplegen. Voor verdere toelichting verwijs ik u graag naar de brief die als bijlage is bijgevoegd waarin ik hierop uitgebreider in ga.

Overig

Wat betreft uw verzoek onder de kop overige deel ik u mede dat uw Kamer inmiddels via het verslag van de bijeenkomst van de Raad Justitie en Binnenlandse Zaken van 8 en 9 maart 2018 is geïnformeerd, zoals hieronder weergegeven.

De Raad hield een oriënterend debat over de interoperabiliteit tussen de EU informatiesystemen. De aanwezige Ministers bevestigden dat de elementen in de Commissievoorstellen aan de behoeften van de lidstaten voldoen. De Commissie deed een zeer sterk beroep op de lidstaten om de ambitieuze agenda te verwezenlijken met een algemene benadering voor de zomer en afronding voor het einde van 2018. Het Europees Parlement zou bereid zijn hieraan mee te werken.
Wat betreft de antwoorden op de vier voorliggende vragen, kan ik u aangeven dat die in lijn zijn met het Nederlandse standpunt zoals aangegeven in het BNC-fiche en in dit schrijven.