Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2022–2023

36 348 Voorstel voor een verordening betreffende vooraf te verstrekken passagiersgegevens met het oog op de controles aan de buitengrenzen I Voorstel voor een verordening betreffende vooraf te verstrekken passagiersgegevens met het oog op het voorkomen van terroristische misdrijven en ernstige criminaliteit

B

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 6 juni 2023

De leden van vaste commissie voor Justitie en Veiligheid[1] hebben in hun commissievergadering van 11 april 2023 beraadslaagd over de door de Europese Commissie voorgestelde voorstellen met nieuwe regels over vooraf te verstrekken passagiersgegevens (Advance Passenger Information – API) om het beheer van de buitengrenzen te vergemakkelijken[2] en de interne veiligheid te vergroten[3] en de BNC-fiches van de regering.[4] De leden van de fracties van **GroenLinks**, **PvdA** en **D66** gezamenlijk hebben kennisgenomen van de BNC-fiches. Zij hebben een aantal vragen met betrekking tot de impact van de voorstellen op de persoonlijke levenssfeer van reizigers en over de effectiviteit van de voorgestelde maatregelen. Ook de leden van de fractie van de **PVV** hebben een aantal vragen.

Naar aanleiding hiervan is op 19 april 2023 een brief gestuurd aan de Minister van Justitie en Veiligheid.

De Minister heeft op 2 juni 2023 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Justitie en Veiligheid,
Van Dooren

---

[1] Samenstelling:
Backer (D66), De Boer (GL) (*voorzitter*), Van Dijk (SGP), Van Hattem (PVV), Rombouts (CDA), Baay-Timmerman (50PLUS), Van den Berg (VVD), Arbouw (VVD), Bezaan (PVV), De Blécourt-Wouterse (VVD), Dittrich (D66), Doornhof (CDA), Janssen (SP), Karimi (GL), Meijer (VVD), Nicolaï (PvdD), Otten (Fractie-Otten) (*ondervoorzitter*), Recourt (PvdA), Rietkerk (CDA), Veldhoen (GL), Van Wely (Fractie-Nanninga), Nanninga (Fractie-Nanninga), Raven (OSF), Karakus (PvdA), Talsma (CU), Hiddema (Fractie-Frentrop) en Krijnen (GL).

[2] COM(2022) 729.

[3] COM(2022) 731.

[4] *Kamerstukken II* 2022/23, 22 112, nr. 3608 en *Kamerstukken II* 2022/23, 22 112, nr. 3609.

kst-36348-B
ISSN 0921 - 7371
's-Gravenhage 2023

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR JUSTITIE EN VEILIGHEID

Aan de Minister van Justitie en Veiligheid

Den Haag, 19 april 2023

De leden van vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 11 april 2023 beraadslaagd over de door de Europese Commissie voorgestelde voorstellen met nieuwe regels over vooraf te verstrekken passagiersgegevens (Advance Passenger Information – API) om het beheer van de buitengrenzen te vergemakkelijken[5] en de interne veiligheid te vergroten[6] en de BNC-fiches van de regering.[7] De leden van de fracties van **GroenLinks**, **PvdA** en **D66** gezamenlijk hebben met belangstelling kennisgenomen van de BNC-fiches. Zij hebben enkele vragen met betrekking tot de impact van de voorstellen op de persoonlijke levenssfeer van reizigers en over de effectiviteit van de voorgestelde maatregelen. Ook de leden van de fractie van de **PVV** hebben een aantal vragen.

Vragen van de leden van de fracties van GroenLinks, PvdA en D66 gezamenlijk

Noodzakelijkheid en effectiviteit

Veel van de bevoegdheden die in de voorstellen zijn opgenomen zijn al onderdeel van het huidige wettelijk kader, maar zijn niet verplicht en/of worden niet overal gelijk toegepast. Hoe waardeert u de meerwaarde en effectiviteit van deze voorstellen met het oog op de verplichting die hiermee wordt geïntroduceerd? Indien lidstaten geen gebruik maakten van de eerdere bevoegdheden, betekende dit dan niet dat ze dergelijke verzameling en verwerking van gegevens onnodig achtten? Zo ja, waarom zouden deze lidstaten hier nu toe verplicht worden?

Ten aanzien van het voorstel rechtshandhaving geeft de Europese Commissie in de toelichting aan dat het gebruik van API-gegevens voor de bestrijding van criminaliteit en terrorisme al mogelijk is onder de huidige PNR-richtlijn. Kunt u naar aanleiding hiervan verder uiteenzetten wat dan nog de meerwaarde van dit voorstel is?

Hanteren centrale router voor overdracht API-gegevens

De leden lezen dat het instellen van een centrale «router» voor het uitwisselen van de API-gegevens een belangrijk onderdeel is van de voorstellen.[8] Hoe beoordeelt u het risico dat een dergelijk centraal uitwisselingspunt of centrale database een aantrekkelijk doelwit wordt voor cybercriminelen of kwaadwillende statelijke actoren? Neemt u dergelijke risico's mee in uw afweging of de uitwisseling en verwerking van API-gegevens zoals voorgesteld een niet te grote inbreuk zijn op de privacy van de betrokken reizigers? Welke andere mogelijke risico's ziet u bij het hanteren van een centrale router voor de overdracht van API-gegevens? Op basis van welke factoren beoordeelt u of deze centrale router voldoende beveiligd zal zijn en zijn deze factoren volledig kenbaar op het moment van besluitvorming? Op welke wijze vindt na realisatie controle plaats op de kwaliteit van de werkelijk gerealiseerde beveiliging?

---

[5] COM(2022) 729.
[6] COM(2022) 731.
[7] *Kamerstukken II* 2022/23, 22 112, nr. 3608 en *Kamerstukken II* 2022/23, 22 112, nr. 3609.
[8] *Kamerstukken II* 2022/23, 22 112, nr. 3609, p. 3.

Verder worden in het voorstel rechtshandhaving geen specifieke databeschermingsmaatregelen genoemd. De leden vragen zich af welke databeschermingsmaatregelen genomen gaan worden, zodat Nederland voldoet aan de verplichtingen die het heeft onder Europees recht?

Criteria voor vluchtenselectie en screening

Kunt u uitleggen op basis van welke criteria wordt geselecteerd voor welke intra-EU vluchten API-gegevens worden verzameld? En hoe voorkomt u dat deze criteria kunnen worden aangemerkt als discriminatoir?

Verder wordt er ten aanzien van de rechtsbescherming gesproken over een risicoanalyse op basis van «objectieve» criteria om te bepalen wie voorafgaand aan de vluchtaankomst gescreend wordt. Kunt u deze criteria verder toelichten en ook hoe wordt voorkomen dat burgers nadelige consequenties ervaren van deze criteria? Op welke wijze wordt voorkomen dat een vals positieve melding een reiziger treft? Is er altijd menselijke toetsing op een computer gegenereerde uitkomst en waaruit bestaat die toetsing? Is het hele gedigitaliseerde proces inzichtelijk voor de toetser, zodanig dat de menselijke tussenkomst ook betekenisvol kan zijn?

Bewaartermijn van gegevens

De Europese Commissie geeft in haar toelichting op het voorstel voor API verordening rechtshandhaving aan dat de PNR-richtlijn zoals uitgelegd door het Hof van Justitie in zaak C-817/19[9] van toepassing is op de bewaartermijnen van API-gegevens onder de nieuwe verordening. In het BNC-fiche van dit voorstel geeft de regering aan dat dit niet specifiek terugkomt in de bepalingen van het voorstel en dat het graag nadere verduidelijking ziet ten aanzien van dit punt. De Autoriteit Persoonsgegevens onderstreept het belang van deze wettelijke bewaartermijnen voor persoonsgegevens in haar van brief van 21 februari 2023 aan u als Minister van J&V. Is er inmiddels duidelijkheid over de bewaartermijnen van API-gegevens onder de verordening rechtshandhaving? Zo ja, wat zijn deze bewaartermijnen precies onder de nieuwe verordening?

Specifiek geeft u in een reactie op de oproep van de Autoriteit Persoonsgegevens aan dat de gegevens van niet geselecteerde vluchten direct worden verwijderd, maar dat de passagiersgegevens van deze niet geselecteerde vluchten bij de relevante luchtvaartmaatschappijen nog wel kunnen worden opgevraagd, in lijn met de relevante bepalingen uit het Wetboek van Strafvordering.[10] Kunnen deze gegevens dan ook worden opgevraagd buiten de driejarentermijn?

De regering geeft aan aandacht te zullen vragen voor uitzonderlijke gevallen waarbij het nodig is om de data langer te bewaren ten behoeve van de bestrijding van illegale migratie en de grenspassage, bijvoorbeeld het geval wanneer API-gegevens gebruikt moeten worden voor het verifiëren van nationaliteit, identiteit en reisroute bij mogelijke asielaanvragen van derdelanders op de luchthaven. Welke criteria hanteert u bij het vaststellen hiervan en is de regering voornemens hier ook een maximumtermijn voor te hanteren?

---

[9] HvJ EU arrest van 21 juni 2022 in zaak C-817/19, *Ligue des droits humains.*

[10] Brief Minister van J&V, *Reactie op de oproep van de Autoriteit Persoonsgegevens,* d.d. 10 maart 2023, kenmerk 4536425.

Verenigbaarheid met hoger recht

In de BNC-fiches voor beide voorstellen wordt aangegeven dat de voorstellen geacht worden in overeenstemming te zijn met de Europese verdragen, het Grondrechtenhandvest en de Nederlandse Grondwet. Het Hof van Justitie van de Europese Unie (hierna: het HvJ EU) heeft in haar uitspraak in de zaak C-817/19 echter stevige kritiek geuit op de voorganger van de voorgestelde verordeningen, namelijk de PNR-richtlijn.[11] Kunt u aangeven op welke wijze de kritiekpunten van het HvJ EU zijn geadresseerd en daarbij een waardering geven of en zo ja, waarom dit afdoende is?

De regering stelt voorstander te zijn van het verzamelen van API-gegevens binnen het grondgebied van de EU om zo illegale en secundaire migratie te bestrijden. Wat kan met API-gegevens wat niet kan met de huidige wijze van gegevensverzameling en uitwisseling? Hoe duidt u het feit dat dit niet in het Commissievoorstel grensbewaking is opgenomen? Komt dit doordat de Commissie het verzamelen van API-gegevens in dit kader niet noodzakelijk, effectief of proportioneel acht? Op basis waarvan maakt u hierin een andere weging dan de Commissie?

Rechtsbescherming

Op welke wijze en voor welke rechter kan een burger opkomen tegen een beslissing die is genomen op basis van API-gegevens? Welke informatie krijgt een burger? Is het voor hem of haar inzichtelijk op basis waarvan de beslissing is genomen en is het (hierdoor) mogelijk een adequaat verweer te voeren? Wordt het de burger ook gemeld als de beslissing op basis van algoritmische besluitvorming heeft plaatsgevonden en welke criteria daarbij zijn gehanteerd?

In het geval is komen vast te staan dat ten onrechte API-gegevens zijn gebruikt bij een besluit, op welke wijze wordt dan gegarandeerd dat de burger hier geen nadeel van zal ondervinden? Geldt deze bescherming voor alle EU-landen in gelijke mate? Is ook gegarandeerd dat in de toekomst geen nadeel meer zal ontstaan voor deze burger, bijvoorbeeld omdat de onjuiste gegevens of conclusies niet overal zijn verwijderd en in andere gegevensbestanden of met andere artificiële intelligentie (AI) op basis van die gegevens toch, en dan niet of zeer moeilijk traceerbaar, tot onterechte negatieve gevolgen voor die burger zullen leiden?

Vragen van de leden van de fractie van de PVV

Op pagina 4 van het BNC-fiche «API verordening grensbewaking» lezen de leden: *«De Commissie stelt voor de maximale termijn voor het bewaren van de gegevens door luchtvaartmaatschappijen en grensbewakingsautoriteiten vanaf het vertrek van de vlucht te verruimen naar 48 uur, omdat de huidige bewaartermijn van 24 te kort is om in alle gevallen pre-checks effectief uit te voeren (in het bijzonder bij langeafstandsvluchten). Daarna moeten de gegevens onmiddellijk en permanent verwijderd worden.»*[12] Naar aanleiding hiervan vragen de leden van de PVV-fractie hoe wordt gewaarborgd en afgedwongen dat de gegevens onmiddellijk en permanent worden verwijderd.

Op pagina 5 van het BNC-fiche staat het volgende: *«Momenteel ontvangt KMar al API-gegevens van alle vluchten inkomend van buiten de EU en EU-lidstaten buiten het Schengengebied naar Nederland. Geautomati-*

[11] HvJ EU arrest van 21 juni 2022 in zaak C-817/19, *Ligue des droits humains.*
[12] *Kamerstukken II* 2022/23, 22 112, nr. 3608, p. 4.

seerde verwerking van passagiersgegevens voorafgaand aan de grenspassage biedt de mogelijkheid sneller, nauwkeuriger en gerichter controles uit te voeren.»[13]
Welke personele veranderingen worden doorgevoerd bij Koninklijke Mareschaussee om in te springen op voorliggend beleid?

Op pagina 6 van het BNC-fiche zijn de volgende passages vermeld: *«Voor rechtshandhavings-doeleinden mogen API-gegevens daarnaast intra-EU worden verzameld. Het kabinet is er voorstander van om dit ook voor grensbewakingsdoeleinden mogelijk te maken, met het oog op het gebruik van API-gegevens van vluchten binnen het grondgebied van de EU om illegale en secundaire migratie te bestrijden. (...)*

Gezien de vroegtijdige verstrekking van API-data aan grensbewakingsautoriteiten de grenspassage kan versnellen zal het kabinet tijdens de onderhandelingen onderzoeken of het mogelijk is deze verstrekking ook te benutten voor andere vervoersmodaliteiten, zoals trein- en busverkeer dat veelal intra-EU is, mede in het licht van klimaatdoelstellingen.»[14] Kunt u een zo gedetailleerd mogelijke toelichting geven inzake «mede in het licht van klimaatdoelstellingen»?

Op pagina 7 van het BNC-fiche lezen de leden van de PVV-fractie: *«Het kabinet staat positief tegenover het voorstel van de Commissie om gebruik te maken van een router voor de doorgifte van API-gegevens. Met de komst van de router verdwijnen de thans in gebruik zijnde verbindingswegen van de luchtvaarmaatschappijen naar de bevoegde autoriteiten van alle verschillende lidstaten op basis van de API-Richtlijn. (...)*

Het kabinet zal aandacht vragen voor de randvoorwaarden die nodig zijn bij het gebruik van de router, zoals de beschikbaarheid en kwaliteit van de verbinding en een back-up bij technische storingen.»[15] Is uitgebreid onderzocht wat de gevolgen voor informatieveiligheid en privacy kunnen zijn (mede in het licht van mogelijke hacks en misbruik) en hoe deze zaken zo goed mogelijk gewaarborgd kunnen worden?

Op pagina 10 van het BNC-fiche lezen de leden van de PVV-fractie: *«Het voorstel met betrekking tot de router zal primair via de EU-begroting moeten worden bekostigd. Dat laat onverlet dat de aansluiting op deze voorziening door lidstaten bijvoorbeeld ICT-matige (hardware en software) gevolgen zal hebben en dat naar verwachting werkprocessen zullen moeten worden aangepast. Dat kan ook leiden tot kosten voor Nederland, die nog nader in kaart moeten worden gebracht. Er wordt geen ruimte voorzien in de nationale programma's ISF en BMVI om deze kosten mede te financieren. Budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.»*[16] Kunt u een eerste schatting geven van de kosten voor Nederland?

De leden van de PVV-fractie ontvangen op bovenstaande vragen graag een gemotiveerd antwoord.

---

[13] *Kamerstukken II* 2022/23, 22 112, nr. 3608, p. 5.
[14] *Kamerstukken II* 2022/23, 22 112, nr. 3608, p. 6.
[15] *Kamerstukken II* 2022/23, 22 112, nr. 3608, p. 7.
[16] *Kamerstukken II* 2022/23, 22 112, nr. 3608, p. 10.

De leden van de vaste commissie voor Justitie en Veiligheid zien uw reactie – bij voorkeur binnen vier weken – met belangstelling tegemoet.

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
M.M. de Boer

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 2 juni 2023

Hierbij stuur ik u mede namens de Staatssecretaris van Justitie en Veiligheid de antwoorden op de op 19 april 2023 ingediende Eerste Kamervragen van de leden van de fracties van Groenlinks, PvdA, D66 en PVV over de BNC-fiches inzake de Advance Passenger Information ontwerpverordeningen.

-

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

Vragen van de leden van de fracties van GroenLinks, PvdA en D66 gezamenlijk

Noodzakelijkheid en effectiviteit

Veel van de bevoegdheden die in de voorstellen zijn opgenomen zijn al onderdeel van het huidige wettelijk kader, maar zijn niet verplicht en/of worden niet overal gelijk toegepast. Hoe waardeert u de meerwaarde en effectiviteit van deze voorstellen met het oog op de verplichting die hiermee wordt geïntroduceerd? Indien lidstaten geen gebruik maakten van de eerdere bevoegdheden, betekende dit dan niet dat ze dergelijke verzameling en verwerking van gegevens onnodig achtten? Zo ja, waarom zouden deze lidstaten hier nu toe verplicht worden?

Het kabinet verwelkomt dit voorstel van de Commissie voor de herziening van de Advance Passenger Information (API-)Richtlijn, zoals ook toegelicht in het BNC-fiche API Grensbewaking. Uit het impact assessment van de Commissie is gebleken dat de huidige API-richtlijn herzien wordt om meer duidelijkheid te bieden aan o.a. nationale autoriteiten en luchtvaartmaatschappijen vanwege de ongelijke implementatie van de API-richtlijn door lidstaten, bijvoorbeeld ten aanzien van de reikwijdte en gegevensbeschermingsvereisten, de interoperabiliteit en bevordering van datakwaliteit. De huidige richtlijn laat aan de lidstaten zelf over om een verplichting op te leggen om API-gegevens aan te leveren en de wijze waarop. Uit de evaluatie van de API-richtlijn in 2020 is gebleken dat het overgrote deel van de lidstaten gebruik maakt van de mogelijkheden die de richtlijn biedt, maar in verschillende mate en op verschillende wijze. De Commissie constateert dat dit onder andere het gevolg is van de complexiteit van de implementatie.

Dat leidt tot een ongelijke datakwaliteit omdat de verificatie en daarmee de juistheid van API-data bepalend is voor het al dan niet aanhouden van de juiste passagier. Ik hecht daarom groot belang aan de verplichting aan luchtvaartmaatschappijen API-data aan te leveren. De geautomatiseerde verwerking van passagiersgegevens voorafgaand aan de grenspassage biedt de mogelijkheid sneller, nauwkeuriger en gerichter controles uit te voeren. Ik vind het tevens belangrijk dat de EU-informatie-uitwisselingprocessen effectief en efficiënt zijn waardoor eindgebruikers zoals grensbewakingsambtenaren sneller en volledieger informatie beschikbaar hebben om hun taken te kunnen uitoefenen. Een goede kwaliteit van informatie is voor het kabinet een essentiële voorwaarde voor het gebruik van systemen en het uitwisselen van informatie, passend bij de mogelijkheden van de betreffende informatiebron en bijbehorende juridische kaders.

Ten aanzien van het voorstel rechtshandhaving geeft de Europese Commissie in de toelichting aan dat het gebruik van API-gegevens voor de bestrijding van criminaliteit en terrorisme al mogelijk is onder de huidige PNR-richtlijn. Kunt u naar aanleiding hiervan verder uiteenzetten wat dan nog de meerwaarde van dit voorstel is?

Het klopt dat de Passenger Name Record (PNR-)dataset op basis van de huidige PNR-richtlijn ook alle verzamelde API-gegevens bevat. Het gaat hierbij echter alleen om gegevens voor zover luchtvaartmaatschappijen die verzamelen voor hun eigen bedrijfsdoeleinden en omvat daarmee geen verplichting voor luchtvaartmaatschappijen om deze gegevens te verzamelen. Daarnaast is volgens de Commissie ook een veiligheid-slacune ontstaan doordat API-gegevens momenteel niet op alle vluchten worden verzameld waar PNR-gegevens worden verzameld (namelijk niet op intra-EU en uitgaande vluchten). Met het voorstel voor de

API-gegevens verordening rechtshandhaving beoogt de Commissie dit gat te dichten.

In tegenstelling tot PNR-gegevens (die de passagier in de regel zelf invult) worden API-gegevens, die afkomstig zijn uit de vertrekcontrole- en check-in-systemen van luchtvaartmaatschappijen, gecontroleerd en geverifieerd. Zo wordt op het moment van inchecken door vergelijking van de passagiersgegevens met het reisdocument van de passagier de identiteit gecontroleerd. Het gecombineerde gebruik van API-gegevens met PNR-gegevens biedt meerwaarde omdat het de betrouwbaarheid van PNR-gegevens vergroot doordat geverifieerde gegevens over de identiteit wordt toegevoegd. Het stelt bevoegde nationale autoriteiten daardoor beter in staat de identiteit van passagiers te bevestigen. Hierdoor zijn de gegevens van meer nut in opsporingsonderzoeken en wordt het risico beperkt dat onschuldige personen onderdeel uitmaken van een controle of onderzoek. Ik zie daarom duidelijke meerwaarde in het voorstel.

Hanteren centrale router voor overdracht API-gegevens

De leden lezen dat het instellen van een centrale «router» voor het uitwisselen van de API-gegevens een belangrijk onderdeel is van de voorstellen. Hoe beoordeelt u het risico dat een dergelijk centraal uitwisselingspunt of centrale database een aantrekkelijk doelwit wordt voor cybercriminelen of kwaadwillende statelijke actoren? Neemt u dergelijke risico's mee in uw afweging of de uitwisseling en verwerking van API-gegevens zoals voorgesteld een niet te grote inbreuk zijn op de privacy van de betrokken reizigers? Welke andere mogelijke risico's ziet u bij het hanteren van een centrale router voor de overdracht van API-gegevens? Op basis van welke factoren beoordeelt u of deze centrale router voldoende beveiligd zal zijn en zijn deze factoren volledig kenbaar op het moment van besluitvorming? Op welke wijze vindt na realisatie controle plaats op de kwaliteit van de werkelijk gerealiseerde beveiliging?

In zowel het Dreigingsbeeld Statelijke Actoren 2022 als het Cybersecuritybeeld Nederland 2022 is geconstateerd dat de digitale integriteit van Nederland en de EU onder druk staat door statelijke actoren. Ook uit het jaarverslag van de AIVD 2022 blijkt dat verschillende landen met offensieve cyberprogramma's in 2022 probeerden data te stelen in de (Europese) reis- en luchtvaartsector. Ze zoeken vooral grote datasets. De Europese Commissie erkent dit in de concept-verordening door aan te geven dat het verwerken van PNR- en API-gegevens op zichzelf risico's met zich meebrengt, omdat deze informatie ook interessant is voor criminelen en kwaadwillende statelijke actoren. De Europese Commissie geeft aan dat juist daarom moet worden voorzien in één enkele router die op het niveau van de Unie wordt opgezet en geëxploiteerd en die dient als verbindings- en distributiepunt voor die doorgifte. Meerdere verbindingen en koppelpunten brengen namelijk meer veiligheidsrisico's met zich mee dan een centrale router. Daarbij is belangrijk dat de router voor API-gegevens geen centrale database is, maar een doorgeefluik voor de doorgifte van luchtvaartmaatschappijen aan de bevoegde autoriteiten van de lidstaten. De gegevens worden alleen voor de duur van die doorgifte in de router bewaard op het niveau van de router, waardoor de risico's beperkter zijn. Desondanks acht ik het van belang dat er voor de centrale router zeer strenge veiligheidsmaatregelen getroffen worden, waarin wordt voorzien zoals hieronder beschreven.

In de concept API-verordeningen is uitgebreid geregeld hoe de informatiebeveiliging wordt ingericht. eu-LISA is verantwoordelijk voor de beveiliging van de API-gegevens die het op grond van de twee API-voorstellen door middel van de router doorgeeft, in het bijzonder API-gegevens die

persoonsgegevens zijn. De bevoegde grensautoriteiten en de luchtvaartmaatschappijen zorgen voor de beveiliging van de API-gegevens die ze op grond van deze verordening verwerken, in het bijzonder de persoonsgegevens. Deze verantwoordelijkheid verandert dus niet ten gevolge van de instelling van de router. eu-LISA, de bevoegde grensautoriteiten en de luchtvaartmaatschappijen werken, overeenkomstig hun respectieve verantwoordelijkheden en met inachtneming van het Unierecht, samen om die beveiliging te waarborgen.

eu-LISA neemt met name de nodige maatregelen om de beveiliging van de router en de via de router doorgezonden API-gegevens te waarborgen. Het agentschap doet dit onder meer door een beveiligingsplan, een bedrijfscontinuïteitsplan en een uitwijkplan op te stellen, uit te voeren en regelmatig te actualiseren. De verordening schrijft voor dat er na de realisatie van de router regelmatig audits inzake de bescherming van persoonsgegevens moeten plaatsvinden. De Europese Toezichthouder voor gegevensbescherming zorgt ervoor dat ten minste eenmaal per jaar overeenkomstig de desbetreffende internationale auditnormen een audit wordt uitgevoerd van de verwerkingsactiviteiten die eu-LISA verricht met betrekking tot API-persoonsgegevens. De bevoegde nationale gegevensbeschermingsautoriteiten zorgen ervoor dat ten minste om de vier jaar overeenkomstig de desbetreffende internationale auditnormen een audit wordt uitgevoerd van de verwerkingsactiviteiten die de bevoegde grensautoriteiten verrichten met betrekking tot API-persoonsgegevens.

Verder worden in het voorstel rechtshandhaving geen specifieke databeschermingsmaatregelen genoemd. De leden vragen zich af welke databeschermingsmaatregelen genomen gaan worden, zodat Nederland voldoet aan de verplichtingen die het heeft onder Europees recht?

Op de verwerking van API-gegevens door luchtvaartmaatschappijen is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De daaropvolgende verwerking van API-gegevens door de Passagiersinformatie-eenheden vindt plaats onder de vereisten en waarborgen die zijn opgenomen in de PNR-Richtlijn en uitgelegd door het Hof van Justitie van de Europese Unie (HvJEU). Eventuele verdere verwerking van de gegevens door nationale rechtshandhavingsautoriteiten moet voldoen aan de voorwaarden van de PNR-Richtlijn en de Richtlijn politie- en justitiegegevens. Daarnaast verplicht het voorstel luchtvaartmaatschappijen logs bij te houden van de datum, het tijdstip en de plaats van de overdracht van de API-gegevens. De logs moeten tot één jaar na creatie bewaard worden, na afloop van deze termijn moeten de logs verwijderd worden tenzij zij nodig zijn voor procedures voor het bewaken of waarborgen van de veiligheid en integriteit van de API-gegevens of de rechtmatigheid van de verwerkingen. In dat geval moeten de logs onmiddellijk en permanent verwijderd worden als zij niet meer nodig zijn voor die doelen.

Criteria voor vluchtenselectie en screening

Kunt u uitleggen op basis van welke criteria wordt geselecteerd voor welke intra-EU vluchten API-gegevens worden verzameld? En hoe voorkomt u dat deze criteria kunnen worden aangemerkt als discriminatoir?

De Commissie heeft rekening gehouden met de uitspraak van het Hof van Justitie van de Europese Unie aangaande de PNR-richtlijn. De doorgifte van API-gegevens is alleen mogelijk voor geselecteerde vluchten binnen de EU, indien die lidstaten ook een grondslag hebben om PNR-gegevens voor die vluchten te ontvangen. Zoals beschreven in mijn brief van

10 maart 2023 aan de Tweede Kamer is naar aanleiding van de uitspraak van het Hof, op basis van objectieve criteria, een risicoanalyse uitgevoerd voor Nederlandse luchthavens. De analyse richt zich op de vraag voor welke vluchten die verband houden met bepaalde luchthavens, er inderdaad aanwijzingen bestaan die het verwerken van intra-EU-passagiersgegevens rechtvaardigen. Hierbij wordt uitgegaan van het risiconiveau van luchthavens binnen Nederland voor die strafbare feiten die passen in de doelbinding van het PNR-instrument. Op basis van objectieve criteria, zoals het aantal verstrekkingen van PNR-gegevens aan bevoegde instanties, gebruikte modus operandi en relevantie voor opsporingsonderzoek, wordt geoordeeld dat passagiersgegevens van intra-EU vluchten van en naar de geselecteerde luchthavens relevant zijn (noodzakelijk) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Deze wijze van selectie zal ook worden toegepast op de API-gegevens.

De criteria zijn nooit gebaseerd op bijzondere persoonsgegevens zoals iemands godsdienst of levensovertuiging, ras of etnische afkomst, politieke gezindheid, gezondheid, seksuele leven of geaardheid of lidmaatschap van een vakvereniging. De «Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven» kent geen grondslag om dergelijke bijzondere persoonsgegevens te verzamelen en/of te verwerken. Mochten bijzondere persoonsgegevens onverhoopt toch door een luchtvaartmaatschappij worden aangeleverd, zijn technische maatregelen genomen om deze gegevens eruit te filteren en direct geautomatiseerd te verwijderen.

Verder wordt er ten aanzien van de rechtsbescherming gesproken over een risicoanalyse op basis van «objectieve» criteria om te bepalen wie voorafgaand aan de vluchtaankomst gescreend wordt. Kunt u deze criteria verder toelichten en ook hoe wordt voorkomen dat burgers nadelige consequenties ervaren van deze criteria? Op welke wijze wordt voorkomen dat een vals positieve melding een reiziger treft? Is er altijd menselijke toetsing op een computer gegenereerde uitkomst en waaruit bestaat die toetsing? Is het hele gedigitaliseerde proces inzichtelijk voor de toetser, zodanig dat de menselijke tussenkomst ook betekenisvol kan zijn?

Het voorstel API Grensbewaking ziet toe op het gebruik van API-gegevens ter verbetering en de bevordering van externe grenscontroles en het tegengaan van irreguliere migratie en worden verstuurd aan het Targeting Center Borders van de Koninklijke Marachaussee (KMar). Het voorstel API Rechtshandhaving betreft het gebruik van API-gegevens ten behoeve van het voorkomen, opsporen, onderzoeken en vervolgen van ernstige criminaliteit en terrorisme en worden verstuurd aan de Passagiersinformatie-eenheid (Pi-NL).

De KMar vergelijkt de gegevens vervolgens met opsporingsregisters, watchlists en profielen en kijkt verder naar passagiers met ongebruikelijke combinaties van persoons- en vluchtkenmerken die kunnen wijzen op irreguliere migratie. De aanpak is daarbij getrapt. De eerste stap is het zoeken naar gesignaleerde passagiers. Vervolgens kan worden bekeken of aan deze passagiers, andere passagiers gelinkt kunnen worden. Daarna wordt gezocht naar opvallende combinaties van persoons- en vluchtkenmerken die mogelijk wijzen op irreguliere migratie. Wanneer sprake is van een «positieve melding» ofwel een zogenoemde «hit» vindt een beoordeling plaats of een interventie gewenst is door de KMar. Bij deze beoordeling hanteert de KMar het vier-ogen-principe: in principe zijn altijd twee mensen betrokken bij de beoordeling van een hit. Wanneer na deze check een extra controle van de betreffende passagier opportuun wordt

geacht, wordt een interventiebericht opgesteld, een zogenaamde API-alert.

De Pi-NL ontvangt alleen de passagiersgegevens, zoals opgenomen in de limitatieve lijst van bijlage 1 van de «Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven»». De Pi-NL beoordeelt de passagiersgegevens om terrorisme en ernstige criminaliteit te bestrijden onder andere aan de hand van risicocriteria sets. Deze risicocriteria sets komen tot stand door analyse van PNR-gegevens, criminaliteitsanalyses en andere relevante opsporingsinformatie. De criteria worden altijd getoetst op juridische en privacyaspecten en vooraf getest, met als doel de hoogst mogelijke nauwkeurigheid ervan te bepalen. De officier van justitie geeft daarbij toestemming voor het inzetten van de risicocriteria set en weegt daarbij proportionaliteit en subsidiariteit. Indien een set van risicocriteria in gebruik wordt genomen, worden in een vooraf bepaalde tijdperiode passagiersgegevens vergeleken met deze criteria – en met de gestelde drempelwaarde die aan de verschillende criteria is gesteld. De Passagiersinformatie-eenheid Nederland deelt de passagiersgegevens of het resultaat van de verwerking ervan, met de bevoegde instanties, indien deze nader onderzoek behoeven.

Verstrekkingen aan bevoegde instanties vinden niet geautomatiseerd plaats, maar pas na een menselijke toets. Dit is een objectieve toets waarbij door een medewerker van de Pi-NL wordt nagegaan of het gaat om een rechtmatige verstrekking van passagiersgegevens binnen de doelbinding van de wet. Daarnaast wordt door een medewerker van de Pi-NL getoetst of de te verstrekken gegevens passen bij het verzoek, signalering of risicocriteria set. Hierbij is het hele gedigitaliseerde proces inzichtelijk voor de toetser.

De PNR-wet kent daarnaast nog een aantal strikte waarborgen voor het beschermen van onschuldige passagiers en de zorgvuldige omgang met hun gegevens. Zo kent de wet een strikte doelbinding, namelijk de bestrijding van ernstige criminaliteit en terrorisme, en is een aparte functionaris voor gegevensbescherming voor de Pi-NL aangesteld.

Bewaartermijn van gegevens

De Europese Commissie geeft in haar toelichting op het voorstel voor API verordening rechtshandhaving aan dat de PNR-richtlijn zoals uitgelegd door het Hof van Justitie in zaak C-817/19 van toepassing is op de bewaartermijnen van API-gegevens onder de nieuwe verordening. In het BNC-fiche van dit voorstel geeft de regering aan dat dit niet specifiek terugkomt in de bepalingen van het voorstel en dat het graag nadere verduidelijking ziet ten aanzien van dit punt. De Autoriteit Persoonsgegevens onderstreept het belang van deze wettelijke bewaartermijnen voor persoonsgegevens in haar van brief van 21 februari 2023 aan u als Minister van J&V. Is er inmiddels duidelijkheid over de bewaartermijnen van API-gegevens onder de verordening rechtshandhaving? Zo ja, wat zijn deze bewaartermijnen precies onder de nieuwe verordening?

De Europese Commissie heeft tijdens de eerste besprekingen van het voorstel in EU-verband bevestigd dat de verwerking van API-gegevens verzameld op basis van de API verordening rechtshandhaving, zal plaatsvinden op basis van de PNR-Richtlijn zoals uitgelegd door het Hof van Justitie in zaak C-817/19.

Met betrekking tot de bewaartermijn oordeelde het Hof dat een bewaartermijn van zes maanden noodzakelijk en proportioneel wordt geacht,

maar dat een langere bewaartermijn slechts beperkt is toegestaan waarbij, kort samengevat, de noodzakelijkheid leidend is. In de brief van 10 maart aan de Tweede Kamer kondig ik de inperking van de algemene bewaartermijn naar drie jaar aan. In lijn met het arrest blijft in specifieke gevallen vijf jaar indien een concrete link met terrorisme of ernstige criminaliteit is gebleken. Nederland zet zich ondertussen in op Europees niveau voor een eenduidige interpretatie van de Hofuitspraak, ook ten aanzien van bewaartermijnen.

Specifiek geeft u in een reactie op de oproep van de Autoriteit Persoonsgegevens aan dat de gegevens van niet geselecteerde vluchten direct worden verwijderd, maar dat de passagiersgegevens van deze niet geselecteerde vluchten bij de relevante luchtvaartmaatschappijen nog wel kunnen worden opgevraagd, in lijn met de relevante bepalingen uit het Wetboek van Strafvordering. Kunnen deze gegevens dan ook worden opgevraagd buiten de driejarentermijn?

De Algemene verordening gegevensbescherming (AVG) is van toepassing op de verwerking van persoonsgegevens door luchtvaartmaatschappijen. Luchtvaartmaatschappijen moeten op grond van een eigen afweging gebaseerd op de AVG bepalen of het, gelet op de doeleinden waarvoor deze passagiersgegevens worden verwerkt, nodig is om die gegevens te bewaren en voor welke tijdsduur. Het betreft namelijk gegevens die zij ten behoeve van de eigen bedrijfsvoering verwerken, en het staat los van de vraag of het gaat om gegevens die wel of niet betrekking hebben op geselecteerde vluchten. Opsporingsinstanties kunnen in die zin proberen, op grond van het Wetboek van Strafvordering, die gegevens te vorderen bij een luchtvaartmaatschappij. Het is dus mogelijk dat de gegevens buiten de driejarentermijn worden gevorderd. Daarbij is het echter wel de vraag of de luchtvaartmaatschappij die gegevens dan nog heeft.

De regering geeft aan aandacht te zullen vragen voor uitzonderlijke gevallen waarbij het nodig is om de data langer te bewaren ten behoeve van de bestrijding van illegale migratie en de grenspassage, bijvoorbeeld het geval wanneer API-gegevens gebruikt moeten worden voor het verifiëren van nationaliteit, identiteit en reisroute bij mogelijke asielaanvragen van derdelanders op de luchthaven. Welke criteria hanteert u bij het vaststellen hiervan en is de regering voornemens hier ook een maximumtermijn voor te hanteren?

Nederland is er voorstander van om in uitzonderlijke categorieën ten behoeve van de bestrijding van illegale migratie API-gegevens langer dan 48 uur te bewaren. Het gaat hierbij om de langere opslag tot vier dagen in geval van verhoogd risico op illegale migratie bij hoog-risico nationaliteiten; en in geval van een API-alert (naar aanleiding van een signalering op basis van risicocriteria en/of databanken) voor de periode van maximaal één jaar.

Verenigbaarheid met hoger recht

In de BNC-fiches voor beide voorstellen wordt aangegeven dat de voorstellen geacht worden in overeenstemming te zijn met de Europese verdragen, het Grondrechtenhandvest en de Nederlandse Grondwet. Het Hof van Justitie van de Europese Unie (hierna: het HvJ EU) heeft in haar uitspraak in de zaak C-817/19 echter stevige kritiek geuit op de voorganger van de voorgestelde verordeningen, namelijk de PNR-richtlijn. Kunt u aangeven op welke wijze de kritiekpunten van het HvJ EU zijn geadresseerd en daarbij een waardering geven of en zo ja, waarom dit afdoende is?

Voor de volledigheid wijs ik uw Kamer erop dat de PNR-richtlijn niet de voorganger is van de voorgestelde verordeningen, maar naast deze API-verordeningen zal blijven bestaan. De voorgestelde verordeningen vervangen wel de bestaande API-richtlijn uit 2004.

Ik verwelkom dat de Commissie in het voorstel reeds rekening heeft gehouden met de uitspraak van het Hof inzake de PNR-richtlijn. Zo kan er alleen sprake zijn van de doorgifte van API-gegevens aan de passagiersinformatie-eenheden van de lidstaten voor een door elke lidstaat opgestelde lijst met geselecteerde vluchten binnen de EU. Het selecteren van álle vluchten binnen de EU, is conform het arrest alleen mogelijk indien de betrokken lidstaat met een werkelijke en actuele of voorzienbare terroristische dreiging wordt geconfronteerd. Daarnaast wordt met het instellen van de centrale router gewaarborgd dat de selectie van vluchten op het niveau van de router plaatsvindt en API-gegevens van niet-geselecteerde vluchten onmiddellijk verwijderd worden. De Europees Toezichthouder voor Gegevensbescherming heeft in haar opinie over de API-voorstellen bevestigd dat deze werkwijze in lijn is met het arrest.

Ik ben van mening dat de Europese Commissie in haar voorstellen voldoende tegemoet komt aan het arrest van het Hof. Dit laat onverlet dat, zoals hierboven beschreven, Nederland zich zal blijven inzetten op Europees niveau voor eenduidige interpretatie van het arrest, ook ten aanzien van de bewaartermijnen. In mijn brief van 10 maart 2023 aan de Tweede Kamer geef ik opvolging aan de uitspraak van het Hof voor het PNR-instrument. Deze interpretatie lijkt te passen bij de interpretatie die de Europese Commissie aan de Hofuitspraak geeft in het kader van de voorgestelde API-verordeningen.

De regering stelt voorstander te zijn van het verzamelen van API-gegevens binnen het grondgebied van de EU om zo illegale en secundaire migratie te bestrijden. Wat kan met API-gegevens wat niet kan met de huidige wijze van gegevensverzameling en uitwisseling? Hoe duidt u het feit dat dit niet in het Commissievoorstel grensbewaking is opgenomen? Komt dit doordat de Commissie het verzamelen van API-gegevens in dit kader niet noodzakelijk, effectief of proportioneel acht? Op basis waarvan maakt u hierin een andere weging dan de Commissie?

Het huidige voorstel voor de API-verordening heeft onder andere tot doel de informatie-uitwisseling ten behoeve van de grensbewaking te verbeteren. Gezien de grensoverschrijdende aard hiervan kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Daarom is een EU-aanpak nodig. Met dit voorstel wordt tevens beoogd de grensoverschrijdende informatie-uitwisseling te verbeteren. Dergelijke harmonisatie kan ook het beste plaatsvinden op EU-niveau. De Commissie heeft echter ervoor gekozen om de verzameling van API-gegevens voor grensbewakingsdoeleinden beperkt te houden tot inkomende vluchten van buiten de EU en Schengen. Voor rechtshandhavingsdoeleinden mogen API-gegevens wél intra-EU worden verzameld. Het kabinet is er voorstander van om dit ook voor grensbewakingsdoeleinden mogelijk te maken, met het oog op het gebruik van API-gegevens van vluchten binnen het grondgebied van de EU om illegale en secundaire migratie te bestrijden. Door toepassing van API-gegevens op vluchten binnen de EU kunnen de grensbewakingsautoriteiten nationale en Europese databanken raadplegen met het oog op het voorkomen van illegale migratie, grensoverschrijdende migratiecriminaliteit en epidemische risico's conform onder andere het voorstel voor de nieuwe Schengengrenscode, waarbij de toegang voor raadpleging noodzakelijk en evenredig dient te zijn. Het intra-Schengengebruik van API-gegevens

zal de autoriteiten van de lidstaten een extra middel geven om het doeltreffende beheer van irreguliere en secundaire migratiebewegingen te verbeteren. Bovendien zal het meer informatie verstrekken over irreguliere reisroutes binnen de EU. Daarom ziet het kabinet meerwaarde in een verbreding van de reikwijdte van het voorstel naar vluchten binnen het grondgebied van de EU. In overeenstemming met de relevante jurisprudentie moet dit worden georganiseerd op een manier die het vrije verkeer niet verstoort en geen formele grenscontrole vormt, noch dat effect heeft, in lijn met voornoemd arrest van het Hof van Justitie van de EU inzake de toepassing van de PNR-Richtlijn op intra-EU vluchten. Daaruit volgt ook dat de verzameling van API-gegevens voor vluchten binnen de EU niet systematisch (voor alle vluchten) kan plaatsvinden.

Rechtsbescherming

Op welke wijze en voor welke rechter kan een burger opkomen tegen een beslissing die is genomen op basis van API-gegevens? Welke informatie krijgt een burger? Is het voor hem of haar inzichtelijk op basis waarvan de beslissing is genomen en is het (hierdoor) mogelijk een adequaat verweer te voeren? Wordt het de burger ook gemeld als de beslissing op basis van algoritmische besluitvorming heeft plaatsgevonden en welke criteria daarbij zijn gehanteerd?

De algemeen toepasselijke rechtshandelingen van de EU zijn van toepassing overeenkomstig de daarin gestelde voorwaarden. Wat de verwerking van persoonsgegevens betreft, gaat het dan met name om de AVG. De voorstellen voor de API-verordeningen laten de toepassing van de AVG onverlet. In de AVG staan, behoudens uitzonderingen, de rechten van betrokkenen, waaronder het recht op informatie, inzage en correctie. De betrokkene heeft ook het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming wanneer dit rechtsgevolgen voor hem heeft of het hem anderszins in aanzienlijke mate treft. In dat geval heeft hij recht op menselijke tussenkomst. Wanneer gegevens bij de betrokkene worden verzameld, dient de in artikel 13, eerste tot en met derde lid, AVG genoemde informatie aan de betrokkene te worden verschaft. Indien de persoonsgegevens niet van betrokkenen zijn verkregen, dient de in artikel 14, eerste, tweede en vierde lid, genoemde informatie te worden verstrekt. In bepaalde gevallen gelden de informatieverplichtingen op grond van artikel 13, vierde lid, en artikel 14, vijfde lid, niet. Het gaat daar met name om de situatie dat betrokkenen reeds over de informatie beschikt. De AVG bevat bepalingen over het toezicht op de naleving. De betrokkene heeft het recht een klacht in te dienen bij de functionaris gegevensbescherming en/of de toezichthouder en op een doeltreffende voorziening in rechte tegen de verwerkingsverantwoordelijke.

In het geval is komen vast te staan dat ten onrechte API-gegevens zijn gebruikt bij een besluit, op welke wijze wordt dan gegarandeerd dat de burger hier geen nadeel van zal ondervinden? Geldt deze bescherming voor alle EU-landen in gelijke mate? Is ook gegarandeerd dat in de toekomst geen nadeel meer zal ontstaan voor deze burger, bijvoorbeeld omdat de onjuiste gegevens of conclusies niet overal zijn verwijderd en in andere gegevensbestanden of met andere artificiële intelligentie (AI) op basis van die gegevens toch, en dan niet of zeer moeilijk traceerbaar, tot onterechte negatieve gevolgen voor die burger zullen leiden?

De betrokkene heeft op grond van artikel 16 van de AVG het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen en het recht op het vervolledigen van onvolledige persoonsgegevens. Artikel 17, eerste lid,

van de AVG bepaalt dat de betrokkene, behoudens uitzonderingen in het derde lid, het recht heeft van de verwerkingsverantwoordelijke zonder onredelijke vertraging verwijdering van hem betreffende persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te verwijderen, onder andere wanneer de persoonsgegevens onrechtmatig zijn verwerkt. Dit recht is met name in het leven geroepen zodat mensen niet voor altijd (ten onrechte) met hun verleden worden geconfronteerd. Naast het zelf verwijderen van de persoonsgegevens dient de verwerkingsverantwoordelijke redelijke maatregelen te nemen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen (artikel 17, tweede lid, van de AVG).

Vragen van de leden van de fractie van de PVV

Op pagina 4 van het BNC-fiche «API verordening grensbewaking» lezen de leden: «De Commissie stelt voor de maximale termijn voor het bewaren van de gegevens door luchtvaartmaatschappijen en grensbewakingsautoriteiten vanaf het vertrek van de vlucht te verruimen naar 48 uur, omdat de huidige bewaartermijn van 24 te kort is om in alle gevallen pre-checks effectief uit te voeren (in het bijzonder bij langeafstandsvluchten). Daarna moeten de gegevens onmiddellijk en permanent verwijderd worden.» Naar aanleiding hiervan vragen de leden van de PVV-fractie hoe wordt gewaarborgd en afgedwongen dat de gegevens onmiddellijk en permanent worden verwijderd.

De Koninklijke Marechaussee verwerkt de API-gegevens volgens de Vreemdelingenwet 2000. Dit geldt voor vluchten vanuit landen die geen lid zijn van de EU noch het Verdrag van Schengen hebben ondertekend. Daarnaast past de Koninklijke Marechaussee in algemene zin de AVG regelgeving toe, met de uitzonderingen die daar gelden bijvoorbeeld ten behoeve van de verdediging van het NL grondgebied en de verwerking van politiegegevens. In de praktijk betekent dit dat de API-persoonsgegevens bij het verstrijken van de bewaartermijn automatisch door het systeem verwijderd worden. Daarop volgt een menselijke check om te controleren of de gegevens daadwerkelijk verwijderd zijn. Indien een reiziger meer informatie wil over zijn of haar rechten op dit terrein is dit online beschikbaar.

Het voorstel voor de API-verordening grensbewaking verplicht de bevoegde nationale autoriteiten voor gegevensbescherming minstens eenmaal per vier jaar audits uit te voeren inzake de verwerking door de grensbewakingsautoriteiten van de API persoonsgegevens in het kader van deze verordening. In Nederland is dit de Autoriteit Persoonsgegevens. Daarbij zal tevens moeten worden gekeken naar het tijdig verwijderen van de API gegevens binnen de termijn van 48 uur. Daarnaast worden de grensautoriteiten geacht ook zelf hun naleving van de verplichtingen onder deze verordening te monitoren, en daarbij in het bijzonder te letten op de verwerking van de API-persoonsgegevens.

Luchtvaartmaatschappijen zijn tevens verplicht de API-persoonsgegevens te verwijderen bij het verstrijken van de bewaartermijn, tenzij deze gegevens nodig zijn voor eigen bedrijfsdoelen. In dat geval is artikel 6 van de AVG van toepassing. De Autoriteit Persoonsgegevens is ook hier de aangewezen toezichthouder.

Op pagina 5 van het BNC-fiche staat het volgende: «Momenteel ontvangt KMar al API-gegevens van alle vluchten inkomend van buiten de EU en

EU-lidstaten buiten het Schengengebied naar Nederland. Geautomatiseerde verwerking van passagiersgegevens voorafgaand aan de grenspassage biedt de mogelijkheid sneller, nauwkeuriger en gerichter controles uit te voeren.
Welke personele veranderingen worden doorgevoerd bij Koninklijke Mareschaussee om in te springen op voorliggend beleid?

In algemene zin kan gesteld worden dat er naar verwachting geen sprake zal zijn van personele veranderingen die uitsluitend toe te wijzen zijn aan de beoogde implementatie van deze API-verordeningen. U wordt nader geïnformeerd over de mogelijke impact te zijner tijd.

Op pagina 6 van het BNC-fiche zijn de volgende passages vermeld: «Voor rechtshandhavings-doeleinden mogen API-gegevens daarnaast intra-EU worden verzameld. Het kabinet is er voorstander van om dit ook voor grensbewakingsdoeleinden mogelijk te maken, met het oog op het gebruik van API-gegevens van vluchten binnen het grondgebied van de EU om illegale en secundaire migratie te bestrijden. (...) Gezien de vroegtijdige verstrekking van API-data aan grensbewakingsautoriteiten de grenspassage kan versnellen zal het kabinet tijdens de onderhandelingen onderzoeken of het mogelijk is deze verstrekking ook te benutten voor andere vervoersmodaliteiten, zoals trein- en busverkeer dat veelal intra-EU is, mede in het licht van klimaatdoelstellingen. 0 Kunt u een zo gedetailleerd mogelijke toelichting geven inzake «mede in het licht van klimaatdoelstellingen»?

Als gevolg van de klimaatdoelstellingen voorziet het kabinet dat internationale treinreizen populairder zullen worden, bijvoorbeeld door het groeiende bewustzijn van de negatieve milieugevolgen van de luchtvaart. Daarnaast zet het Ministerie van Infrastructuur en Waterstaat zich in, samen met Schiphol, KLM, ProRail en NS, voor het verbeteren van de internationale trein als aantrekkelijk alternatief voor de luchtvaart op korte afstanden. Door deze stimulatie, zal naar verwachting reizen per trein en bus toenemen. Het is cruciaal om zicht te hebben op alle reizigersbewegingen in het kader van de bestrijding van illegale en secundaire migratie alsmede van terrorisme en zware criminaliteit. Het is daarom van belang op deze vervoersmodaliteiten API-gegevens ook te kunnen benutten.

Op pagina 7 van het BNC-fiche lezen de leden van de PVV-fractie: «Het kabinet staat positief tegenover het voorstel van de Commissie om gebruik te maken van een router voor de doorgifte van API-gegevens. Met de komst van de router verdwijnen de thans in gebruik zijnde verbindingswegen van de luchtvaarmaatschappijen naar de bevoegde autoriteiten van alle verschillende lidstaten op basis van de API-Richtlijn. (...)

Het kabinet zal aandacht vragen voor de randvoorwaarden die nodig zijn bij het gebruik van de router, zoals de beschikbaarheid en kwaliteit van de verbinding en een back-up bij technische storingen. Is uitgebreid onderzocht wat de gevolgen voor informatieveiligheid en privacy kunnen zijn (mede in het licht van mogelijke hacks en misbruik) en hoe deze zaken zo goed mogelijk gewaarborgd kunnen worden?

Graag verwijs ik u voor dit antwoord naar de reactie op de hierboven gestelde vraag van de fracties D66, PvdA en GL inzake het hanteren van een centrale router voor overdracht API-gegevens.

Op pagina 10 van het BNC-fiche lezen de leden van de PVV-fractie: «Het voorstel met betrekking tot de router zal primair via de EU-begroting moeten worden bekostigd. Dat laat onverlet dat de aansluiting op deze voorziening door lidstaten bijvoorbeeld ICT-matige (hardware en

software) gevolgen zal hebben en dat naar verwachting werkprocessen zullen moeten worden aangepast. Dat kan ook leiden tot kosten voor Nederland, die nog nader in kaart moeten worden gebracht. Er wordt geen ruimte voorzien in de nationale programma's ISF en BMVI om deze kosten mede te financieren. Budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.» 12 Kunt u een eerste schatting geven van de kosten voor Nederland?

Inzake de financiële consequenties kunnen momenteel geen indicaties worden aangegeven. Uw Kamer wordt hierover nader geïnformeerd.