36 158 Regels ter uitvoering van EU-verordeningen op het terrein van grenzen en veiligheid (Uitvoeringswet EU-verordeningen grenzen en veiligheid)

Nota naar aanleiding van het verslag

INHOUDSOPGAVE

I. ALGEMEEN

Met veel belangstelling heeft de regering kennis genomen van de gestelde vragen en gemaakte opmerkingen van de aan het woord zijnde fracties in het verslag bij het onderhavige wetsvoorstel. Er is inbreng is geleverd door de leden van de fracties van de VVD, D66 en de SP. De leden van de VVD-fractie hebben kennis genomen van het voorstel en danken de regering. De leden van de D66-fractie merken op dat de regering vrijwel alle adviezen van de Raad van State heeft overgenomen en hebben slechts enkele vragen. De leden van de CDA-fractie hebben opgemerkt kennis te hebben genomen van het wetsvoorstel en af te zien van een schriftelijke inbreng omdat zij geen nadere vragen hebben. De leden van de SP-fractie geven aan het belang van samenwerking tussen de zogenaamde Schengenlanden op het gebied van criminaliteit, grenzenbeleid, visumbeleid en migratiebeleid te onderschrijven vanwege het wegvallen van interne grenscontroles. Daarbij geven de leden aan dat het uitwisselen van informatie handen en voeten kan geven aan samenwerking op het gebied van criminaliteitsbestrijding, grenzenbeleid, visumbeleid en migratiebeleid, maar dat het wel proportioneel, effectief en subsidiair moet zijn en daarom nog diverse vragen hebben.

De regering gaat in deze nota naar aanleiding van het verslag graag in op de gestelde vragen in de volgorde van het verslag. De gestelde vragen zijn integraal en cursief opgenomen, waarbij de beantwoording van de zijde van de regering onder de vragen die het betreft is opgenomen.

1. Aanleiding

Vragenblok 1 - VVD

De leden van de VVD-fractie willen graag het belang van een goed grensbewakingssysteem benadrukken. Deze leden vragen dan ook welk effect de regering verwacht dat deze verordeningen zullen hebben op de instroom van asielzoekers. Bevatten de verordeningen volgens de regering voldoende drukmiddelen om ervoor te zorgen dat alle EU-lidstaten de verordeningen adequaat uitvoeren? Wat zijn de risico's als enkele lidstaten de verordeningen onvoldoende of te langzaam uitvoeren? Welke mitigerende maatregelen bevatten de verordeningen hiervoor? Deze leden vragen hoe haalbaar de beoogde tijdslijnen zijn voor zowel Nederland als andere lidstaten.

De doelstellingen van de verordeningen betreft het voorkomen van illegale immigratie en beschermen van de veiligheid van het Schengengebied. De doeltreffendheid van de grenscontroles wordt bij de implementatie van de verschillende verordeningen verhoogd. Voor onderdanen van derde landen die naar het Schengengebied willen afreizen kan via het Europees reisinformatie- en autorisatiesysteem (Etias) dan wel via het Visuminformatiesysteem (VIS) worden gemonitord of hun inreis een risico op het gebied van illegale migratie of veiligheid vormt. De risico´s worden deels geput uit de signaleringen in het Schengeninformatiesysteem (SIS). Daarnaast geldt dat een van de doelstellingen van het Entry Exit Systeem (EES) is het mogelijk maken om verblijfsduuroverschrijders te identificeren en op te sporen, en de bevoegde nationale autoriteiten van de lidstaten in staat stellen passende maatregelen te treffen. De systemen kunnen een bijdrage leveren aan het beperken van de instroom van migranten die op illegale wijze het Schengengebied binnenkomen.

Voor wat betreft de drukmiddelen die er zijn om ervoor te zorgen dat alle lidstaten de EU-verordeningen adequaat uitvoeren geldt in ieder geval dat net als voor andere Europeesrechtelijke verplichtingen de Europese Commissie bij niet naleving van deze verplichtingen een inbreukprocedure kan starten tegen de betreffende lidstaat. Indien noodzakelijk kan de Commissie de zaak vervolgens voor het Hof van Justitie van de EU brengen. Daarnaast bevatten de verordeningen mechanismen om te monitoren hoe de werking van de verordeningen verloopt in de vorm van terugkerende evaluaties. Op deze wijze blijft ook na ingebruikname van de systemen in beeld hoe de werking van de verordeningen verloopt.

Voor Nederland is het net als voor andere lidstaten essentieel dat kwalitatief hoogwaardige centrale Europese systemen tijdig beschikbaar komen, zodat er voldoende tijd is voor het nationale test- en implementatietraject. Nederland heeft ongeveer 7 maanden implementatietijd nodig ná oplevering van een kwalitatief uitstekend en stabiel centraal systeem door eu-LISA (“European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice”). Deze voorwaarde is gedeeld met de Europese Commissie en eu-LISA. Daarnaast is er een afhankelijkheid van andere lidstaten, aangezien elk afzonderlijke systeem simultaan in alle lidstaten in werking zal treden. Wanneer één lidstaat niet gereed is, zal de inwerkingtreding worden uitgesteld. In Nederland is in 2018 besloten tot de opzet van een programma om de implementatie te begeleiden. Met de implementerende partners is binnen het programma besloten dat de Europese planning leidend is voor de Nederlandse implementatie. Nederland ligt voor de realisatie en implementatie op schema.

De Commissie heeft sinds juni 2020 om de risico’s te mitigeren een Rapid Alert proces opgezet waarmee de voortgang van de implementatie van de IT-systemen bij de lidstaten en het Europese agentschap eu-LISA wordt gemonitord. Op basis van dat mechanisme kan snel gerichte ondersteuning worden geboden. Nederlandse experts zijn vertegenwoordigd in diverse Europese overleggen en expert groepen. Op deze wijze kan veelvuldig worden overlegd en kunnen *best practices* worden uitgewisseld.

Vragenblok 2 - VVD

Gezien het belang van het systeem, is er ook een mogelijkheid op cyberaanvallen die het systeem proberen te ontregelen, zo stellen de leden van de VVD-fractie. Hoe schat de regering de kans op cyberdreigingen en hackpogingen in? Welke veiligheidsmaatregelen worden genomen tegen mogelijke cyberaanvallen op deze systemen? Zijn deze volgens de regering adequaat?

De regering acht de dreiging van cyberaanvallen reëel. Aangezien de potentiele impact groot is moet Nederland zich daar tegen wapenen voor de nationale systemen. Het gaat immers om grote hoeveelheden gevoelige persoonsgegevens. In de verordeningen is dat al ondervangen doordat er een security plan wordt vereist en passende bescherming van persoonsgegevens. Nederland heeft dit securityplan opgesteld.

Naar aanleiding van aanbevelingen van het Adviescollege ICT-toetsing (AcICT) is het securityplan verder aangevuld. De implementatie van maatregelen is onderdeel van alle fasen van de ontwikkeling van de systemen.

Eu-LISA is verantwoordelijk voor de beveiliging van centrale informatiesystemen. Ook daarvoor zijn uitgebreide securityplannen opgesteld. De verordeningen zien ook op periodieke audits van zowel de nationale als de centrale systemen. Volgens de regering wordt met deze maatregelen voorzien in een adequate bescherming van de systemen.

Vragenblok 3 - SP

De leden van de SP-fractie vernemen dat, met de Uitvoeringswet EU-verordeningen grenzen en veiligheid, Nederland gebruik gaat maken van de nieuwe systemen EES en Etias en daarnaast van de nieuwe mogelijkheden van de bestaande systemen VIS en SIS. Bovendien worden deze systemen straks gekoppeld via het zogenaamde European search portal (ESP) waardoor met één bevraging maar liefst acht systemen doorzocht kunnen worden, namelijk de Interpol systemen, de Europol systemen, SIS, EES, Etias, VIS, Eurodac en ECRIS-TCN. Legio verschillende organisaties zal daar toegang toe krijgen, alleen al in Nederland gaat het om diverse organisaties van de Koninklijke Marechaussee tot aan het ministerie van Buitenlandse Zaken, en de verantwoordelijkheid komt ook op diverse plekken te liggen. Het is dus een omvangrijke en complexe wijziging. Toch merken deze leden op dat het uitwisselen van al deze extra gegevens onvoldoende worden toegelicht. Wat is daar de ratio achter? Gaan al die autoriteiten nu echt de juiste gegevens uitwisselen die nu nog niet bekend zijn of creëert Europa zeeën aan data waar geen behoefte aan is en niemand het overzicht van kan houden? Welke waarborgen dienen er eigenlijk bij het uitwisselen van al deze gegevens? Als laatste vragen deze leden naar een reflectie van de regering op het toeslagenschandaal. Via het koppelen van allerlei gegevens werden personen ten onrechte verdacht gemaakt en zelfs gestraft. Hoe wordt dit voorkomen met de enorme bak aan gegevens die hier gaat ontstaan?

De totstandkoming van de verschillende verordeningen waar het wetsvoorstel op ziet kent een lange voorgeschiedenis waarbij een aantal tekortkomingen in de toen bestaande Europese informatiesystemen op het terrein van grenzen en veiligheid werd gesignaleerd. In 2016 presenteerde de Commissie een mededeling over krachtigere en slimmere informatiesystemen voor grenzen en veiligheid, waarin deze tekortkomingen aan bod kwamen, zoals een suboptimale werking van de systemen, lacunes in informatiebeheer, een complex landschap van op verschillende wijze beheerde systemen en een gefragmenteerde architectuur van gegevensbeheer voor grenstoezicht en veiligheid. In 2017 bracht een deskundigengroep verslag uit waarin voorstellen werden gedaan om de tekortkomingen aan te pakken door het optimaliseren van de bruikbaarheid van de bestaande informatiesystemen, het waar nodig ontwikkelen van aanvullende systemen om informatielacunes op te vullen en het waarborgen van de interoperabiliteit van de systemen. Aanbevelingen waren onder meer om één zoekportaal te ontwikkelen voor alle systemen, één gezamenlijke dienst voor biometrische matching en één gemeenschappelijk identiteitsregister. De deskundigengroep heeft ook aanbevolen om nader te kijken naar ‘gaten’ in doelgroepen. Zo is onder andere gewezen op houders van een visum lang verblijf of personen met een verblijfsvergunning en illegale vreemdelingen die geen asielverzoek hebben ingediend.

De verordeningen waar het wetsvoorstel op ziet zijn het resultaat van deze voorgeschiedenis om een oplossing te bieden voor de geconstateerde tekortkomingen.

Het uitwisselen van gegevens draagt bij aan een beter beheer van de buitengrens van het Schengengebied en zorgt voor een verhoogde interne veiligheid binnen de Europese Unie. Door betere informatie-uitwisselingen worden belangrijke lacunes op veiligheidsgebied gedicht.

Daarnaast wordt er door de uitwisseling van gegevens een bijdrage geleverd aan de correcte identificatie van personen en het ondersteunen van de doelstellingen van de verschillende onderdelen. Interoperabiliteit zorgt ervoor dat deze Unie-informatiesystemen en de hierin opgenomen gegevens elkaar aanvullen, met inachtneming van de grondrechten van het individu.

Een van de interoperabiliteitscomponenten omvat het European Search Portal (ESP). Hierdoor worden alle systemen in één keer doorzoekbaar, waarbij door de verschillende gebruikers van de uitvoeringsorganisaties rekening wordt gehouden met de verschillende toegangsrechten tot de centrale EU-informatiesystemen. Het verkrijgen van toegang voor een nationale autoriteit is afhankelijk van wat het juridisch kader van het onderliggende systeem hierover regelt. Het is dus niet zo dat iedere autoriteit via het ESP toegang krijgt tot alle systemen. Dit hangt namelijk af van de rechten die die specifieke autoriteit heeft. Die rechten zijn gebaseerd op de specifieke taak die

de betreffende autoriteit heeft en dan ook beperkt tot wat nodig is voor de uitvoering van die taak. Dit gebeurt aan de hand van gebruikersprofielen die vastleggen tot welke gegevens toegang kan worden verkregen. De personeelsleden van de autoriteiten die de taak gaan uitvoeren die de verordening aan die autoriteit oplegt dienen naar behoren te worden gemachtigd voor het verkrijgen van toegang tot de systemen overeenkomstig het gebruikersprofiel. Verdergaande verwerking zoals het koppelen van gegevens is niet toegestaan. De verordeningen regelen dan ook dat naast de privacy-rechten die betrokkenen hebben, de lidstaten aansprakelijk zijn voor schade die betrokkenen lijden door onrechtmatige gegevensverwerking of een andere handeling in strijd met de verordening. Andere maatregelen die worden getroffen zien bijvoorbeeld op het loggen van de systemen waaruit onder meer blijkt welke gegevens met welk doel en door welke autoriteit zijn geraadpleegd. Zowel op EU-niveau als op het niveau van de lidstaten wordt voorzien in toezicht op de verwerking van persoonsgegevens, namelijk door respectievelijk de Europese toezichthouder voor gegevensbescherming en de Autoriteit Persoonsgegevens (hierna: AP). Daarbij worden op reguliere basis audits verricht op de gegevensverwerking. Op deze wijze zijn er meerdere mechanismen in werking die onrechtmatige gegevensuitwisseling zoveel mogelijk voorkomen, aan het licht brengen en bestraffen.

De leden van de SP-fractie wijzen verder op het Toeslagenschandaal en vragen om een reflectie van de regering hierop. Bij de Europese systemen geldt dat deze worden gereguleerd door de verordeningen, die duidelijk regelen welke autoriteiten wanneer toegang krijgen tot de systemen. Zoals hierboven aan bod kwam is verdergaande verwerking zoals het koppelen van gegevens niet toegestaan. Doordat de Europese wetgever heeft gekozen voor een systematiek zoals hierboven beschreven waarbij toegang beperkt is en er diverse controlemechanismen zijn, is de bescherming van de personen van wie gegevens worden verwerkt tegen onrechtmatige verwerking gewaarborgd. Daarnaast geldt dat de verordeningen de rechten van betrokkenen uitgebreid reguleren voor wat betreft de bescherming van persoonsgegevens. Hierop zal nog nader worden ingegaan in de vragenblokken 27 en volgende.

Vragenblok 4 - SP

De leden van de SP-fractie achten het waardevol dat via het bevragen van het ESP snel kan worden geïdentificeerd welke lidstaat relevante gegevens heeft over de betrokken personen. Hebben deze leden het goed begrepen dat alle systemen werken via een zogenaamd hit/no-hit systeem waardoor nooit rechtstreeks alle inhoudelijke informatie zichtbaar is, maar alleen welke lidstaat relevante gegevens over die persoon heeft in het kader van één van de systemen of verschilt dit per systeem? Indien lidstaten wel gelijk de gegevens in krijgen te zien, meent de regering dat dit proportioneel is?

De verordeningen werken zo dat er sprake is van gedifferentieerde toegangsrechten tot de systemen, afhankelijk van de taak van de betreffende bevoegde autoriteit en het doel waarvoor toegang wordt verleend. Indien een bevoegde autoriteit verantwoordelijk is voor de invoer van gegevens in een van de systemen, gaan de toegangsrechten verder dan als er sprake is van het raadplegen van een van de systemen voor andere doeleinden, zoals voor rechtshandhavingsdoeleinden.

Het ESP is gekoppeld aan de verschillende systemen zodat deze via dit ESP doorzocht kunnen worden. Daarbij wordt zoals hierboven in vragenblok 3 al even aan bod kwam gebruik gemaakt van profielen die bepalen welke toegangsrechten tot welke systemen een bevoegde autoriteit heeft. Dit profiel is gekoppeld aan de taak die de betreffende autoriteit heeft en gaat niet verder dan dat. Daardoor krijgt de betrokken autoriteit niet meer gegevens te zien dan nodig voor de uitvoering van zijn taak.

Voor het voorkomen, opsporen en vervolgen van terroristische misdrijven en andere ernstige strafbare feiten is het in bepaalde gevallen toegestaan de systemen te raadplegen indien er het vermoeden is dat er gegevens over de betrokkene staan opgeslagen in een van de systemen. In dat geval kan via een hit/no-hit gekeken worden of een van de systemen gegevens bevat. Indien dat inderdaad het geval is volgt er een procedure aan de hand waarvan toestemming kan worden verkregen tot het raadplegen van een de systemen die het betreft.

De verordeningen maken dus onderscheid ten aanzien van welke instantie met welke reden de systemen kan raadplegen voor wat betreft de gegevens die getoond worden. Op deze wijze is de proportionaliteit dan ook gewaarborgd.

Vragenblok 5 - SP

De leden van de SP-fractie beseffen dat bij het verzamelen van gegevens er altijd het risico op function-creep aanwezig. Function-creep betekent dat gegevens voor andere doeleinden worden gebruikt dan waarvoor ze oorspronkelijk zijn verzameld. Kan de regering aangeven waarom zij van mening is of er hier sprake is van function-creep en waarom zij dat wel of niet problematisch vindt nu de systemen VIS en SIS worden uitgebreid?

In reactie op de vragen van de leden van de SP-fractie wil de regering graag benadrukken dat de verordeningen vastleggen welke autoriteiten voor welke doeleinden de systemen mogen raadplegen. Het gebruik van deze systemen en de gegevens die daarin staan voor andere doeleinden is dan ook niet toegestaan. Door het loggen van het raadplegen van de systemen en het toezicht daarop worden de risico's op function-creep zo veel mogelijk geminimaliseerd.

2. EES, Etias en VIS

2.1 De EES-verordening

Vragenblok 6 - VVD

De leden van de VVD-fractie erkennen het belang van de doelstellingen van het EES. Grensbewaking is een essentieel onderdeel van een goed werkend migratiesysteem binnen de EU. Hoe meer dit aan de buitengrenzen van de Schengenzone gebeurt, hoe beter dit is voor de veiligheid van de gehele zone. Deze leden zien het dan ook als positief dat hier stappen in gezet worden middels het EES. Kan de regering verder toelichten hoe dit systeem kan bijdragen aan onderzoek in verband met terrorisme en andere ernstige strafbare feiten?

Voor het EES geldt dat, net als voor Etias en VIS, een van de doelstellingen van de betreffende verordening het bijdragen tot het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten is. Dit vindt plaats door aangewezen autoriteiten, dat wil zeggen de met de opsporing van strafbare feiten belaste ambtenaren, onder voorwaarden toegang te verlenen tot de informatiesystemen. Dit is het geval indien toegang voor raadpleging nodig is met het oog op het voorkomen, opsporen en onderzoeken van een terroristisch misdrijf of een ander ernstig strafbaar feit. De toegang voor raadpleging dient daarnaast noodzakelijk en evenredig te zijn in een specifiek geval en er dient bewijsmateriaal of gegronde redenen te zijn om aan te nemen dat de raadpleging van de EES-gegevens zal bijdragen tot het voorkomen, opsporen of onderzoeken van de desbetreffende strafbare feiten. Dit met name wanneer er een gegrond vermoeden bestaat dat de verdachte, de dader of het slachtoffer van een terroristisch misdrijf of een ander ernstig strafbaar feit behoort tot een van de personen die in het EES worden geregistreerd.

Vragenblok 7 - SP

De leden van de SP-fractie begrijpen dat met de EES de in- en uitreisbewegingen van derdelanders worden geregistreerd. Tevens worden verzoeken om personen te weigeren opgenomen net als gezichtsopnamen. Het systeem moet het stempelen van paspoorten bij de grensovergang gaan vervangen, al blijft die optie wel mogelijk. Gaat Nederland ook het afstempelen van paspoorten vervangen? En hebben deze leden het goed begrepen dat het systeem ook vingerafdrukken afneemt van derdelanders die vrijgesteld zijn van de visumplicht? Kan de regering toelichten wat het nut is van die vingerafdrukken en waarom dat specifiek voor deze groep geldt? Gaat Nederland ook vingerafdrukken afnemen wanneer bijvoorbeeld iemand die aan de bovenstaande eisen voldoet via Schiphol Schengen betreedt?

Met de wijziging van de Schengengrenscode (SGC) in verband met de invoering van het EES wordt het verplicht om het stempelen van paspoorten te vervangen door registratie in het EES. De optie om het stempelen in paspoorten te handhaven is van tijdelijke aard doordat deze ziet op de eerste periode van invoering van het EES. Daarnaast is voorzien in overgangsmaatregelen voor lidstaten die het EES nog niet gebruiken. Nederland zal dan ook overeenkomstig de wijziging van de SGC het afstempelen van paspoorten vervangen.

Het klopt dat het afnemen van vingerafdrukken gaat plaatsvinden voor onderdanen van derde landen die worden toegelaten voor kort verblijf en zijn vrijgesteld van de visumplicht. Van onderdanen van derde landen die visumplichtig zijn worden in het kader van de visumprocedure al vingerafdrukken afgenomen, waardoor het afnemen van vingerafdrukken van deze doelgroep niet nogmaals nodig is. Het afnemen van vingerafdrukken heeft als doel om personen correct te identificeren en identiteitsfraude tegen te gaan. Deze verplichtingen volgen uit de verordeningen en gelden ongeacht de plaats waar de inreis plaatsvindt, dus ook op Schiphol.

2.2 De Etias-verordening

Vragenblok 8 - VVD

De leden van de VVD-fractie hebben begrepen dat systemen als Etias al in gebruik zijn in landen als de Verenigde Staten en Australië. Wat zijn de overeenkomsten en verschillen tussen deze systemen en Etias en welke lessen kunnen wij hiervan leren?

Vanuit Europa is met de ontwikkeling van Etias opdracht gegeven aan PricewaterhouseCoopers (PwC) om een haalbaarheidsstudie uit te voeren. Daarin zijn systemen uit VS, Canada en Australië vergeleken met de opzet van het Etias.[1] De systemen voor Etias, de ESTA uit de VS, eTA uit Canada en eTA uit Australië hebben als overeenkomst dat er een aanvraag moet worden gedaan voorafgaand aan een reis naar het betreffende land of zone om een mate van zekerheid te krijgen over de toegang. Het geeft echter in geen van de landen recht op toegang, de toegang wordt door de grenswachter bij de grenspassage beoordeeld. De doelstelling van de verschillende reisautorisaties is gelegen in het voorafgaand aan het afreizen naar de bestemming bepalen of er redenen zijn de derdelander te weigeren. De opzet is daarmee op hoofdlijnen gelijk aan die van de aanvragen in de VS, Canada en Australië. Een belangrijk verschil tussen ESTA en Etias betreft de rechtsmiddelen. Waar de VS geen mogelijkheid biedt om een procedure te starten tegen een weigering van de ESTA, kent de Europese regelgeving rondom Etias wel de mogelijkheid om rechtsmiddelen in te zetten tegen een Etias-besluit. Australië en ook Canada bieden de mogelijkheid een rechtsmiddel aan te wenden bij afwijzing. De Europese wetgever heeft dit rapport betrokken bij de verdere ontwikkeling van Etias.

Vragenblok 9 - SP

De leden van de SP-fractie begrijpen dat met de oprichting van het Etias-systeem inreizigers van het Schengengebied vooraf kunnen worden gescreend in het kader van veiligheid, illegale migratie en epidemische risico's. Zo kan personen voorafgaand aan hun boottocht of vlucht eventueel de toegang tot Schengen worden ontzegd. Dit roept echter diverse vragen op. Hoe en wie beoordeelt of een persoon op basis van veiligheidsrisico's de toegang tot Schengen moet worden ontzegd? Klopt het dat hier altijd, in ieder geval in Nederland, een officier van justitie tussenstaat of mag de Koninklijke Marechaussee, die belast is met de grensbewaking, een dergelijk besluit zelfstandig nemen? En op basis waarvan? En waarom is er voor Etias en tevens voor de andere gegevensbanken niet gekozen het voor te leggen aan de rechter-commissaris?

Een aanvraag voor een reisautorisatie wordt eerst op automatische wijze verwerkt door het centrale Etias-systeem, waarbij onder meer het SIS wordt gecontroleerd op relevante signaleringen, het VIS op het weigeren van een visum en bijvoorbeeld op het bestaan van een overeenkomst met een door de Commissie opgestelde risico-indicator. Deze indicatoren worden onder meer opgesteld

[1] https://home-affairs.ec.europa.eu/system/files/2020-09/etias_feasability_study_en.pdf

aan de hand van statistieken voor illegale immigratie of hoog epidemiologisch risico. Indien deze automatische verwerking geen hit oplevert krijgt een persoon automatisch een reisautorisatie.

Indien het Etias-systeem wel een hit signaleert, wordt de aanvraag handmatig verwerkt door de centrale Etias-eenheid (dus op Europees niveau). De centrale Etias-eenheid verifieert eerst of de hits en de gegevens kloppen. Bij een valse hit wordt alsnog een reisautorisatie afgegeven en worden de gegevens gecorrigeerd. Indien de hit wel klopt wordt de aanvraag doorgezet naar de verantwoordelijke nationale Etias-eenheid die de aanvraag inhoudelijk beoordeelt. In bepaalde gevallen zal de nationale Etias-eenheid in ieder geval de reisautorisatie weigeren, namelijk als a) het voor de aanvraag gebruikte reisdocument overeenkomt met een reisdocument dat in SIS staat geregistreerd als verloren, gestolen, verduisterd of ongeldig verklaard en b) de aanvrager in SIS is gesignaleerd met het oog op weigering van inreis en verblijf. De Etias-verordening regelt dat er in andere gevallen een beoordeling plaatsvindt door de nationale Etias-eenheid van het risico voor de veiligheid of het risico van illegale immigratie. Daarbij wordt onder meer gebruik gemaakt van risico-indicatoren en de informatie uit de hits. Eventueel kan worden verzocht om aanvullende informatie of documentatie van de aanvrager, andere lidstaten of Europol. De nationale Etias-eenheid beslist op basis van deze informatie zelfstandig over de afgifte van een reisautorisatie. Indien deze beoordeling resulteert in een weigering van de reisautorisatie kan de aanvrager in bezwaar tegen deze beslissing, gevolgd door beroep bij de rechter.

De aanvraag voor een reisautorisatie betreft de aanvraag voor een bestuursrechtelijk besluit, waartegen bezwaar en beroep open staat. De rechter-commissaris heeft een rol in het strafrechtelijk domein, wat hier niet aan de orde is. Het gaat hier namelijk om een besluit dat samenhangt met het verlenen van toegang tot Schengen voor onderdanen van derde landen en niet om de opsporing en vervolging van strafbare feiten. Om die reden is er dan ook geen rol weggelegd voor de rechter-commissaris en is dit door de regering ook niet overwogen.

Vragenblok 10 - SP

Hebben de leden van de SP-fractie het goed begrepen dat wanneer een grensbewaker buiten Nederland het ESP bevraagt over een derdelander en er een hit opduikt die is ingevoerd door een Nederlandse autoriteit, dat de Nederlandse Etias National Unit de vraag moet beantwoorden of die derdelander toegang moet krijgen tot Schengen? Of is het zo dat de betreffende grensbewaker op basis van informatie van de Nederlandse Etias National Unit een beslissing moet maken?

De centrale Etias-eenheid beoordeelt welke nationale Etias-eenheid verantwoordelijk is voor een handmatige afdoening. Wanneer een hit op bijvoorbeeld het VIS is ingevoerd door een Nederlandse autoriteit, is de kans groot dat de handmatige afwikkeling van de aanvraag wordt toebedeeld aan de Nederlandse Etias-eenheid. De Nederlandse Etias-eenheid krijgt dan te zien dat er een hit is en kan via de gebruikelijke nationale kanalen de informatie opvragen bij de autoriteiten die de gegevens hebben ingevoerd. Indien de handmatige afwikkeling van de aanvraag is toebedeeld aan een andere lidstaat die ook hits heeft ingevoerd, krijgt die andere lidstaat een melding van de centrale Etias-eenheid dat er een hit is ingevoerd door Nederland. Daarna wordt er door de verantwoordelijke lidstaat een raadplegingsprocedure gestart. Nederland geeft dan een gemotiveerd positief of negatief advies af op basis van de in Nederland bekende gegevens. Daarbij worden de brongegevens (zoals strafdossiers) waarop dit advies is gebaseerd niet gedeeld. Na een negatief advies van een lidstaat, mag de verantwoordelijke lidstaat uitsluitend nog een reisautorisatie afgeven voor zijn eigen territorium.

Vragenblok 11 - SP

Dezelfde vraag geldt voor illegale migratie, zo stellen de leden van de SP-fractie. Kan de regering in de eerste plaats toelichten wat dat betekent? Vallen vluchtelingen die een aanvraag tot asiel in één van de Schengenlanden in willen dienen hier bijvoorbeeld ook onder? Zo ja, hoe wordt het dan mogelijk voor vluchtelingen om nog asielaanvragen in Schengenlanden in te dienen als ze vooraf geen autorisatie meer krijgen om naar de EU af te reizen?

De systemen dragen bij aan het beperken van de instroom van migranten die op illegale wijze het Schengengebied betreden. In het kader van een Etias- of VIS-aanvraag wordt gekeken of er een risico bestaat op illegale immigratie en op vestigingsgevaar. Met de inwerkingtreding van Etias geldt voor visumvrije derdelanders dat zij een Etias-reisautorisatie voorafgaand aan hun reis dienen aan te vragen. Op deze wijze kan bepaald worden of de persoon in aanmerking komt voor toegang tot het Schengengebied, dan wel of zijn inreis een risico met zich meebrengt. Dit omvat tevens het risico op vestiging. Dit risico wordt gebaseerd op bijvoorbeeld het feit dat de aanvrager in het EES geregistreerd staat als een persoon die zijn toegestane verblijfsduur overschrijdt dan wel of de aanvrager in het verleden als zodanig geregistreerd is geweest. Het zal dan ook veel lastiger worden om zonder reisautorisatie naar Nederland af te reizen, aangezien luchtvervoerders, zee-vervoerders en internationale vervoerders die groepen per bus over land vervoeren gehouden zijn om te controleren of reizigers over een reisautorisatie beschikken.

Vanzelfsprekend blijft het mogelijk om conform het Vluchtelingenverdrag en het EU-recht een verzoek tot internationale bescherming te doen. Het aanvragen van asiel wordt door het systeem niet belemmerd.

Vragenblok 12 - SP

Ook de screening op basis van epidemische risico's roept vragen op bij de leden van de SP-fractie. Hoe wordt bepaald of een individu een epidemisch risico vormt voor het Schengengebied? Gebeurt dit aan de hand van risico's op het niveau van landen waarvan de onderdanen toegang wordt ontzegd zoals ten tijde van de coronapandemie gebeurde? Wie moet uiteindelijk de beslissing maken of een reiziger een epidemisch risico vormt en op basis van welke informatie? In hoeverre kan de Koninklijke Marechaussee worden voorbereid op het uitvoeren van deze taak en/of is er al ervaring opgedaan tijdens de coronapandemie?

Een aanvraagdossier moet aan de hand van de Etias-screeningsregels worden geanalyseerd door de in het aanvraagdossier geregistreerde gegevens te vergelijken met specifieke risico-indicatoren voor vooraf bepaalde veiligheidsrisico's, risico's op het gebied van illegale immigratie of hoog epidemiologisch risico's. De Commissie stelt een uitvoeringshandeling vast tot nadere omschrijving van het veiligheidsrisico, het risico op het gebied van illegale immigratie of hoog epidemiologisch risico. Deze uitvoeringshandelingen zijn gebaseerd op door de lidstaten verstrekte informatie over een specifiek hoog epidemiologisch risico, evenals door het Europees Centrum voor ziektepreventie en -bestrijding (ECDC) verstrekte informatie, gebaseerd op epidemiologisch toezicht en risicobeoordelingen, en door de World Health Organization (WHO) gemelde uitbraken van ziekte. Aan de hand van specifieke risico-indicatoren beoordeelt uiteindelijk de nationale Etias-eenheid of een reisautorisatie wordt verleend.

Informatie die is opgegeven bij een aanvraag voor een reisautorisatie, zal altijd eerst geautomatiseerd in het centrale Etias-systeem worden getoetst. Bij eventuele hits daarin, zal in beginsel de nationale Etias-eenheid (ENU) van de lidstaat van eerste inreis deze moeten afhandelen. Dat geldt dus ook voor hits op basis van mogelijk epidemisch risico.

Op grond van artikel 33, eerste lid, van de Etias-verordening zullen door de ETIAS-screeningraad van de centrale Etias-eenheid en screeningsregels een handelswijze worden gecreëerd, bestaande uit specifieke risico-indicatoren voor een epidemisch risico waarmee de informatie van aanvragers zal worden vergeleken. Daarnaast voorziet de Etias-verordening in de oprichting van een onafhankelijke Etias-sturingsraad voor de grondrechten met een advies- en beoordelingsfunctie. De Etias-sturingsraad voor de grondrechten voert regelmatig beoordelingen uit en doet aanbevelingen over de gevolgen voor de grondrechten van de verwerking van aanvragen en van de toepassing van artikel 33, met name wat betreft privacy, bescherming van persoonsgegevens en non-discriminatie.

Hoe voornoemde screeningsregels en handelswijze eruit zullen komen te zien en hoe het proces op nationaal niveau exact zal verlopen, is nog niet bekend. Deze processen zijn nog in ontwikkeling. Binnen Nederland ligt het voor de hand het RIVM hierop te laten adviseren, aangezien het RIVM ook adviseert aan de WHO en ECDC en dat eerder ook tijdens de coronapandemie heeft gedaan. De Koninklijke Marechaussee, waar de nationale Etias-eenheid in Nederland zal worden ondergebracht,

is in afwachting van voornoemde uitvoeringshandeling reeds bezig met de ontwikkeling van een nationaal werkproces, waarbij specifiek wordt gekeken naar eerdere ervaringen bij Corona en Ebola. Daarnaast vindt overleg plaats met ketenpartners als de IND en het ministerie van Buitenlandse Zaken over bij hen vergelijkbare bestaande werkprocessen bij onder andere de beoordeling van visumaanvragen.

Vragenblok 13 - SP

In de memorie van toelichting lezen de leden van de SP-fractie dat veel informatie die in Etias wordt opgenomen tevens in het SIS kan worden geregistreerd. Bij voorkeur dient dan ook het SIS gebruikt te worden, zo schrijft de regering. Wat is dan het nut van Etias als SIS dezelfde informatie herbergt en beide systemen toch tegelijk via het ESP bevraagd kunnen worden?

Het onderdeel waar de leden van de SP-fractie aan refereren betreft een specifiek onderdeel van Etias, namelijk de Etias-observatielijst die kan worden gehanteerd voor het beoordelen van een veiligheidsrisico. Het Etias systeem is, zoals eerder omschreven, een reisinformatie- en autorisatiesysteem, waarmee vóór de reis van niet-visumplichtige onderdanen van derde landen bepaald kan worden of zij in aanmerking komen voor toegang tot het Schengengebied. Het Etias-informatiesysteem verwerkt de ingediende aanvragen en vergelijkt de aanvraaggegevens met signaleringen in onder andere SIS en de Etias-observatielijst. De observatielijst kan worden gebruikt voor het beoordelen van een veiligheidsrisico. Lidstaten beschikken over de mogelijkheid om onderdanen van derde landen op te voeren op een Etias-observatielijst die wordt opgesteld op basis van informatie met betrekking tot terroristische misdrijven of andere ernstige strafbare feiten. In Nederland gaat de voorkeur er naar uit om indien aan de voorwaarden wordt voldaan een signalering in SIS in te voeren en niet een aanmelding uit te voeren voor de Etias-observatielijst. Het uiteindelijke resultaat is hetzelfde omdat bij aanvragen voor een reisautorisatie zowel SIS als de observatielijst worden gecontroleerd.

Vragenblok 14 - SP

De leden van de SP-fractie hebben nog vragen over toegang voor vervoerders tot Etias. Het is uiteraard logisch dat KLM bijvoorbeeld bij het boarden in een derde land vooraf checkt of voor alle reizigers naar Schiphol, dat onderdeel van Nederland is en dus het Schengengebied, autorisatie is verleend om naar Schiphol te reizen. Tegelijk bevat Etias, met daaraan gekoppeld andere databases, bijzondere persoonsgegevens. Tot welke informatie krijgen particuliere vervoerders toegang en welke waarborgen gelden daarbij?

Lucht- en zee-vervoerders en internationale vervoerders die groepen per bus over land vervoeren, wordt de verplichting opgelegd voor het instappen te controleren of de reizigers in het bezit zijn van een geldige reisautorisatie. Vervoerders hebben daarbij geen toegang tot het Etias-dossier zelf, maar kunnen aan de hand van reisdocumentgegevens controleren of een reisautorisatie is afgegeven. Het Etias-informatiesysteem bezorgt de vervoerders door middel van het toegangsportaal een respons “OK/NIET OK” waarbij wordt vermeld of de persoon al dan niet een geldige reisautorisatie heeft. Tot verdere gegevens hebben vervoerders dan ook geen toegang.

2.3 De herziening van de VIS-verordening

Vragenblok 15 - VVD

De leden van de VVD-fractie verwelkomen het dichten van de veiligheidslacune op het gebied van informatie-uitwisseling over visa voor lang verblijf en verblijfsvergunningen. Op welke manier zullen de nieuw toegevoegde doelstellingen ten uitvoer worden gebracht?

Het is juist wat de leden van de VVD-fractie aangeven dat met de herziening van de VIS-verordening een veiligheidslacune wordt gedicht. Aanvragen voor visa voor lang verblijf en verblijfsvergunningen worden voordat de herziening van VIS is doorgevoerd nog niet geregistreerd

in een van de Europese informatiesystemen. Tevens worden de aanvragen nog niet vergeleken met gegevens uit de andere systemen. Met het opnemen van aanvragen voor visa voor lang verblijf en verblijfsvergunningen in VIS wordt dan ook een veiligheidslacune gedicht doordat door de interoperabiliteit met de andere systemen bijvoorbeeld wordt gecontroleerd of een persoon gesignaleerd is in SIS of geregistreerd staat in het EES in verband met het overschrijden van de verblijfsduur.

Daarnaast geldt aan de grens dat vanaf het moment dat de interoperabiliteit van VIS met de andere systemen een feit is, via het Europese zoekportaal (ESP) gebruik gemaakt kan worden van informatie van het EES en het Etias om controles te verrichten. Hierdoor ontstaat een betere en zorgvuldigere informatie-uitwisseling. Het gaat hierbij om verificatie van de identiteit van de houder van het visum, verificatie van de echtheid en de status van het visum en de vaststelling of aan de voorwaarden voor toegang tot het grondgebied van de lidstaten is voldaan. Daarnaast zal zich in de nieuwe constructie veel moeilijker identiteitsfraude voor kunnen doen, bijvoorbeeld doordat onder de nieuwe verordening gebruikt gemaakt gaat worden van gezichtsopnamen ter plekke. Hierdoor zal de mogelijkheid tot *morphing* van foto's worden ondervangen.

Vragenblok 16 - SP

De leden van de SP-fractie begrijpen dat VIS gewijzigd moet worden om deze te kunnen koppelen aan het EES en Etias. Daarnaast zal het VIS ook gewijzigd worden om machtigingen tot voorlopig verblijf en verblijfsvergunningen te registreren. Kan de regering toelichten hoe deze informatie exact bijdraagt aan het bestrijden van terroristische misdrijven en de identificatie van personen?

Voor zowel het EES, als Etias en zowel de huidige VIS-verordening als de VIS-verordening na herziening geldt dat de doelstellingen van deze systemen mede zijn gelegen in het voorkomen, opsporen of onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten. Met de herziening van de VIS-verordening blijft deze doelstelling overeind en wordt de procedure die geldt voor toegang tot het VIS voor rechtshandhavingsdoeleinden gelijk getrokken met de procedure die geldt voor de raadpleging van EES en Etias. De informatie uit het VIS draagt hieraan bij doordat net als bij EES en Etias in bepaalde gevallen met opsporing belaste ambtenaren het VIS mogen raadplegen indien wordt voldaan aan de in de verordening gestelde voorwaarden. Zo moet raadpleging noodzakelijk en evenredig zijn met het oog op het voorkomen, opsporen en onderzoeken van een terroristisch misdrijf of een ander ernstig strafbaar feit in een specifiek geval. Ook dienen er redelijke gronden te zijn om aan te nemen dat de raadpleging van VIS-gegevens wezenlijk zal bijdragen tot het voorkomen, opsporen of onderzoeken van de desbetreffende strafbare feiten, met name indien er een gegrond vermoeden bestaat dat de verdachte, de dader of het slachtoffer van een terroristisch misdrijf of een ander ernstig strafbaar feit behoort tot een van de categorieën waarop de VIS-verordening van toepassing is (artikel 22 sexdecies, eerste lid, van de herziene VIS-verordening). Het centraal toegangspunt controleert of aan de voorwaarden voor toegang wordt voldaan en dient dan ook toestemming te geven.

Ten aanzien van de identificatie van personen die vermist, ontvoerd of als slachtoffers van mensenhandel aangemerkt zijn en ten aanzien van wie er gegronde redenen bestaan om aan te nemen dat de raadpleging van VIS-gegevens zal bijdragen aan hun identificatie, of tot het onderzoek naar specifieke gevallen van mensenhandel geldt een aangepaste procedure (artikel 22 septdecies van de herziene VIS-verordening). In die gevallen is het niet noodzakelijk dat sprake van de hierboven genoemde voorwaarden voor het voorkomen, opsporen of onderzoeken van strafbare feiten.

3. SIS-verordeningen

Vragenblok 17 - SP

De leden van de SP-fractie begrijpen dat SIS wordt ontleend aan drie verschillende verordeningen met elk een eigen doel en grondslag in het Verdrag van de Werking van de EU. Het gaat dan om grenscontroles, terugkeer en politiële en justitiële samenwerking in strafzaken. Hebben deze leden

het echter goed begrepen dat al die gegevens in één gegevensbank terechtkomen? Terwijl die gegevens ook nog eens via het ESP te bevragen is? Een goed terugkeerbeleid is noodzakelijk om het draagvlak voor de opvang van asielzoekers te behouden en tevens om plekken voor asielzoekers vrij te houden. Toch vragen deze leden wat het nut is van deze registratie. Welke autoriteiten kunnen nu de registratie van een terugkeerbesluit inzien en welke actie dienen zij hieraan te koppelen? Wat moet Nederland bijvoorbeeld doen met een Algerijn die in Duitsland voor asiel is afgewezen en tegen wie een terugkeerbesluit is genomen?

SIS betreft weliswaar één informatiesysteem, maar kan worden geraadpleegd voor verschillende doeleinden en kent daardoor verschillende toegangsrechten. De bevoegde autoriteiten, die een taak hebben op het gebied van grenscontroles, terugkeer en politiële en justitiële samenwerking in strafzaken, kunnen het SIS slechts raadplegen voor zover dat noodzakelijk is voor de uitvoering van hun taak. Bijgevolg kunnen niet alle bevoegde autoriteiten alle gegevens raadplegen. De SIS-verordeningen voorzien in nadere regels hierover. Met het ESP kunnen dan ook niet alle autoriteiten alle gegevens in het SIS raadplegen. Voor het raadplegen van SIS is het gebruik van het ESP optioneel. Het ESP kan het Centrale SIS-systeem (C.SIS) bevragen, maar niet het nationale SIS (N.SIS). Op een beperkte categorie gegevens kan worden gezocht in ESP, te weten op personen en documenten gerelateerd aan personen. Het ESP wordt in het kader van interoperabiliteit nog verder ontwikkeld waarbij de architectuur nationaal nog moet worden bepaald. Ook dan zal echter gelden dat autoriteiten alleen die gegevens kunnen raadplegen die voor de uitvoering van hun taken nodig zijn en de betreffende autoriteiten geen toegang hebben tot andere gegevens in het SIS.

De reden dat een terugkeerbesluit in SIS kan worden opgenomen is zodat bijgehouden kan worden welke personen daadwerkelijk Schengen verlaten en welke personen de termijn voor terugkeer overschrijden. Ter uitvoering van de SIS-verordeningen voorziet voorliggend wetsvoorstel in een grondslag voor het raadplegen van het SIS door de nationaal bevoegde autoriteiten, door te verduidelijken welke autoriteiten in Nederland worden bedoeld met de omschrijving die de verordening geeft. Ten aanzien van een terugkeerbesluit geldt dat zulks slechts kan worden geraadpleegd door IND, DT&V, politie en KMar en slechts voor zover dat in een concreet geval noodzakelijk is voor de uitvoering van hun taak.

Bij het gestelde voorbeeld geldt dat, afhankelijk van de concrete situatie, Nederland verschillende dingen moet doen. Daarbij is tevens relevant of de Algerijn zijn terugkeertermijn heeft overschreden. Indien de gesignaleerde Algerijn wordt aangetroffen op bijvoorbeeld Schiphol bij de uitreis uit het Schengengebied, wordt Duitsland als signalerende lidstaat geïnformeerd over de terugkeer. De signalering wordt vervolgens gewist in SIS. Indien van toepassing, bijvoorbeeld omdat de Algerijn buiten zijn terugkeertermijn zit, kan vervolgens een signalering in SIS worden ingevoerd met het oog op weigering van toegang en verblijf. Een soortgelijke procedure geldt indien de Algerijn wordt aangetroffen bij binnenkomt op Schiphol. Duitsland wordt dan geïnformeerd als signalerende lidstaat. Indien er tevens een inreisverbod is opgelegd wordt de signalering in verband met het door Duitsland genomen terugkeerbesluitdoor Nederland gewist en wordt een signalering voor weigering van toegang en verblijf opgenomen. Een andere mogelijkheid is dat indien Nederland een verblijfsvergunning overweegt te verlenen aan de Algerijn en bij het raadplegen van SIS ziet dat Duitsland een signalering inzake terugkeer met een inreisverbod heeft opgelegd, Nederland Duitsland raadpleegt via de uitwisseling van aanvullende informatie. Indien de Algerijn in Nederland wordt aangetroffen in kader van het vreemdelingentoezicht, geldt dat Nederland in deze situatie twee dingen moet doen:

- de signalerende lidstaat – via Bureau SIRENE – informeren dat de vreemdeling in Nederland is aangetroffen, zodat informatieuitwisseling op grond van artikel 7, tweede lid, van de SIS-terugkeerverordening plaatsvindt en;

- bezien of een terugkeerbesluit opgelegd kan worden aan de vreemdeling en of een eventuele inbewaringstelling volgt.

Samengevat dient Nederland in het gestelde voorbeeld de signalerende lidstaat te informeren, SIS bij te werken en eventueel aanvullende acties te ondernemen.

Vragenblok 18 - SP

Het valt de leden van de SP-fractie op dat het SIS ook DNA-profielen kan bevatten. Welke autoriteiten mogen met welk doel deze DNA-profielen opnemen? Kan de regering dat nog eens helder toelichten?

In reactie op de vragen van de leden van de SP-fractie is het goed om voor nadere beantwoording te benadrukken dat dit onderdeel alleen SIS-politiële en justitiële samenwerking in strafzaken betreft en niet raakt aan SIS-grenscontroles of SIS-terugkeer. Daarnaast geldt dat DNA-profielen alleen aan signaleringen mogen worden toegevoegd als het gaat om vermiste personen die in bescherming moeten worden genomen voor hun eigen veiligheid of ter voorkoming van een bedreiging van de openbare orde of de openbare veiligheid, en voorts slechts voor zover foto´s, gezichtsopnames of dactyloscopische gegevens niet beschikbaar zijn of niet geschikt zijn voor identificatie.

Wanneer een DNA-profiel wordt toegevoegd aan een signalering bevat dat profiel enkel de informatie die strikt noodzakelijk is voor de identificatie van de vermiste persoon. Het DNA-profiel wordt slechts gebruikt om de identiteit van de betrokkene te bevestigen van een persoon die naar aanleiding van een alfanumerieke doorzoeking in SIS is gevonden. Een DNA-profiel in SIS kan slechts worden geraadpleegd door ambtenaren van de KMar, politie en openbaar ministerie.

Vragenblok 19 - SP

De leden van de SP-fractie hebben in navolging van de Autoriteit Persoonsgegevens (AP) ook vragen over het aanhouden van de kopie van SIS. De regering betoogt begrijpelijkerwijs dat ook ten tijde van onderhoud aan het systeem of bij storingen de autoriteiten beschikking willen hebben over de meest recente gegevens. Toch sluiten deze leden zich bij de AP aan dat de opslag van gegevens zich tot een minimum moet beperken. Kan de regering nog eens toelichten waarom zij de kopie proportioneel en noodzakelijk vindt?

De verantwoordelijkheid voor het waarborgen van de ononderbroken beschikbaarheid van SIS-gegevens voor de eindgebruikers wordt door de verordeningen neergelegd bij de lidstaten (artikelen 6 van de SIS-verordening politiële en justitiële samenwerking en SIS-verordening grenscontroles en artikel 19 SIS-verordening terugkeer). In deze verordeningen wordt de nationale kopie ook genoemd om als back-up te gebruiken om een ononderbroken beschikbaarheid voor de eindgebruikers te waarborgen. In het verleden heeft Nederland al bewust gekozen voor het hebben van een gehele kopie van C.SIS in verband met de nationale veiligheid en het in eigen hand houden van de beschikbaarheid van SIS-gegevens aan de grens en voor de opsporing. Met de geldende artikelen hierover in de SIS-verordeningen geldt dit des temeer. Naast onderhoud dat eu-LISA pleegt aan het netwerk, heeft Nederland recentelijk nog uitval van C.SIS ervaren waarbij teruggevallen kon worden op de nationale kopie om zodoende geen hits te missen in Nederland. Bij het ontbreken van een kopie kan ook de vergelijking van passagiersgegevens (zogeheten PNR en API-data) met signaleringen niet plaatsvinden ter voorkoming, opsporing en vervolging van zware criminaliteit en terrorisme, met alle mogelijke schade van dien. Daarnaast geldt dat het C.SIS de hoeveelheid zoekopdrachten die Nederland richt tot het N.SIS niet zou kunnen verwerken. Dit is aanvullend een reden dat een kopie bestaat om de continuïteit te waarborgen.

4. Interoperabiliteit

Vragenblok 20 - SP

De leden van de SP-fractie hebben kennisgenomen van het voorstel om naast het inrichten van EES en Etias en het wijzigen van VIS en SIS ook interoperabiliteit tussen deze systemen en andere systemen te bewerkstelligen. Via de ESP kunnen autoriteiten in één keer acht systemen bevragen. Tot welke informatie een beambte toegang heeft hangt af van diens autorisatie. Zo moet de toegang tot gegevens altijd functioneel en proportioneel zijn. Wie ziet erop toe dat dit systeem altijd functioneert, zodat een medewerker van de Immigratie- en Naturalisatiedienst (IND) die

bevoegd is om informatie over een terugkeerbesluit in te voeren, geen toegang krijgt tot bijvoorbeeld medische gegevens in het kader van epidemische risico's in Etias?

Beide verordeningen interoperabiliteit regelen dat de antwoorden die het ESP geeft, uitsluitend de gegevens bevatten waartoe de gebruiker op grond van het Unierecht en het nationale recht toegang heeft. Daardoor zal een gebruiker die krachtens het EU- en Nederlandse recht geen toegang heeft tot bepaalde gegevens, ook niet via een ESP-zoekslag aan die gegevens kunnen komen (artikel 9, vierde en zesde lid).

Voor alle verordeningen geldt dat daarin is vastgelegd welke autoriteiten toegang krijgen voor welke doelstellingen. De lidstaten dienen aan eu-LISA te melden welke autoriteiten dat in de betreffende lidstaat zijn en personeelsleden 'naar behoren te machtigen'. Ten aanzien van het ESP geldt dat er gebruikersprofielen worden opgesteld waaruit de toegangsrechten blijken van deze gebruikers. Deze gebruikersprofielen betreffen in ieder geval:

- de velden die gebruikt kunnen worden voor zoekvragen;
- de EU informatiesystemen, Europol data en Interpol databases die zullen en mogen worden geconsulteerd en die een antwoord teruggeven aan de gebruiker;
- de data die in elk antwoord wordt opgenomen.

De raadpleging van het ESP is daarnaast controleerbaar doordat eu-LISA logbestanden bijhoudt van alle gegevensverwerkingsverrichtingen in het ESP. In deze logbestanden wordt het volgende vermeld: a) de lidstaat die of het Unie-agentschap dat de zoekopdracht start en het gebruikte ESP-profiel; b) de datum en het tijdstip van de zoekopdracht; c) de doorzochte Unie-informatiesystemen en Interpol-databanken. Elke lidstaat houdt vervolgens logbestanden bij van de zoekopdrachten van zijn autoriteiten en van de personeelsleden van zijn autoriteiten die naar behoren gemachtigd zijn om het ESP te gebruiken. Deze logbestanden mogen uitsluitend worden gebruikt voor het toezicht op de gegevensbescherming, onder meer door de toelaatbaarheid van een zoekopdracht en de rechtmatigheid van de gegevensverwerking te controleren, en voor het verzekeren van de gegevensbeveiliging en -integriteit.

Vragenblok 21 - SP

Onderdeel van de interoperabiliteit is ook de shared biometric matching service, zo lezen de leden van de SP-fractie. Dat systeem vergelijkt vingerafdrukken en gezichtsopnames uit de verschillende gegevensbanken met elkaar. Deze informatie wordt geanonimiseerd opgeslagen in een eigen bestand. Kan de regering nog eens toelichten wat het nut hiervan is? Klopt het dat dit alleen het doel dient om te kijken of één persoon niet onder meerdere identiteiten staat geregistreerd? En indien dit het geval is, waarom staat dit dan los van het common identity register? Hebben deze leden het goed begrepen dat die zogenaamde common identity repository ook als onafhankelijke gegevensbank inzichtelijk is voor de politie? Zo ja, wat is daar het nut van? En hoe verhoudt dit zich dan weer tot de multiple identity detector die ook meerdere identiteiten kan signaleren?

Het shared biometric matching service (sBMS) is ingesteld door de beide verordeningen interoperabiliteit ter ondersteuning van het gemeenschappelijk identiteitsregister (het 'common identity register: CIR) en het multiple identity register (MID). Deze drie onderdelen van de verordeningen interoperabiliteit hangen dan ook onlosmakelijk met elkaar samen.

In het CIR worden een aantal gegevens gescheiden per informatiesysteem opgeslagen die afkomstig zijn uit de onderliggende systemen. Van ieder van in een van de systemen geregistreerde persoon wordt een afzonderlijk bestand aangelegd met als doel de correcte identificatie van deze personen. Het gaat dus om de gegevens die zien op de identiteit. Op grond van de EES-verordening worden bijvoorbeeld onder meer naam, nationaliteit, soort en nummer van het gebruikte reisdocument en een gezichtsopname geregistreerd. Deze identiteitsgegevens worden in het CIR geregistreerd. De andere gegevens zoals bijvoorbeeld de datum en tijdstip van inreis van deze persoon, staan in het EES geregistreerd.

De MID is bedoeld om controles mogelijk te maken indien in de onderliggende systemen identiteiten zijn opgenomen die met elkaar verband houden of lijken te houden. Indien er sprake

lijkt te zijn van meerdere identiteiten zorgt de MID voor het aanmaken en opslaan van een identiteitsbevestigingsbestand. Dit bestand bevat links tussen de verschillende informatiesystemen. Indien niet met zekerheid kan worden gesteld dat de gevonden identiteiten horen bij dezelfde persoon wordt een gele link aangemaakt die handmatig wordt geverifieerd door de autoriteit die de gegevens heeft vastgelegd die tot de gele link hebben geleid. Op deze wijze worden de gegevens op juistheid gecontroleerd en fraude opgespoord. De MID bevat zelf dus geen identiteitsgegevens, alleen linkjes met verwijzingen naar identiteitsgegevens. De MID wordt zelf niet door eindgebruikers bevraagd met uitzondering van autoriteiten belast met de handmatige identiteitsverificatie.

Het sBMS is specifiek bedoeld om biometrische gegevens te kunnen vergelijken. Het sBMS slaat biometrische templates op die worden verkregen uit de onderliggende Europese informatiesystemen. Dit maakt het mogelijk om biometrische gegevens die zijn opgeslagen in het CIR met elkaar te vergelijken. Een biometrische template is een mathematische weergave die wordt verkregen door uit biometrische gegevens uitsluitend de kenmerken te extraheren die nodig zijn om identificaties en verificaties te verrichten. De templates bevatten op grond van de verordeningen dus geen biografische identiteitsgegevens en zijn niet terug te herleiden tot linken aan de oorspronkelijke biometrische gegevens zonder toegang tot het onderliggende systeem waar deze gegevens zijn opgeslagen. Met andere woorden, de biometrische gegevens (vingerafdrukken en gezichtsbeelden) worden exclusief bewaard door de onderliggende systemen. De centrale voorziening zal enkel de templates creëren en opslaan met een referentie naar het onderliggende systeem.

De beide verordeningen interoperabiliteit regelen de instelling van dit sBMS omdat biometrische gegevens zoals vingerafdrukken en gezichtsopnames uniek zijn en derhalve voor de identificatie van een persoon veel betrouwbaarder dan alfanumerieke gegevens. De sBMS dient als technisch instrument om het werk van de relevante Europese informatiesystemen en andere interoperabiliteitscomponenten te versterken en vereenvoudigen. Het doel is om de identificatie van een natuurlijk persoon die mogelijk in meerdere van de betreffende informatiesystemen is geregistreerd te vergemakkelijken. De sBMS zorgt ervoor dat één enkel technisch component nodig is om biometrische gegevens te matchen in plaats van meerdere. Dit bevordert de veiligheid en biedt financiële, operationele en onderhouds-technische voordelen. Momenteel heeft elk EU-informatiesysteem dat biometrische gegevens bevat een eigen zoekmachine, ofwel een eigen BMS.

Het sBMS is dus noodzakelijk voor de juiste identificatie van een persoon én maakt het mogelijk meerdere identiteiten tussen de verschillende centrale systemen op te sporen, twee belangrijke doelstellingen van interoperabiliteit. Voor de detectie van meerdere identiteiten wordt door het CIR gebruik gemaakt van het sBMS wanneer het gaat om biometrische gegevens

De leden van SP-fractie hebben goed begrepen dat het CIR in bepaalde gevallen inzichtelijk is voor politieautoriteiten zoals bedoeld in de beide verordeningen interoperabiliteit. Artikel 20 van de beide verordeningen over interoperabiliteit biedt lidstaten de mogelijkheid daarvoor te kiezen. De regering stelt voor hiervan gebruik te maken en verwijst hierbij naar artikel 8 van het wetsvoorstel. Het nut daarvan is dat de politieautoriteiten het CIR dan kunnen raadplegen voor de juiste identificatie van een persoon ter voorkoming en bestrijding van illegale migratie en in het kader van rechtshandhaving of een natuurramp, ongeval of terroristische aanslag. De regering hecht daaraan, omdat de consequenties van geen of foute identificatie groot kunnen zijn. Dit betreft zowel het risico op een verkeerde straf- of vreemdelingenrechtelijke beslissing (bijvoorbeeld een onterechte aanhouding, veroordeling of invrijheidstelling of toewijzing of afwijzing van een aanvraag) als het risico voor een derde wiens identiteit wordt gebruikt. Als een zoekslag in het CIR ertoe kan bijdragen om bij twijfel over identiteit of onmogelijkheid om te identificeren, te identificeren en vergissingen, anonimiteit of identiteitsfraude tegen te gaan, dienen wat de regering betreft de mogelijkheden te worden aangegrepen die het EU-recht daarvoor biedt.

De raadpleging van het CIR door de politieautoriteiten ziet dus niet op de goede werking van de systemen zelf maar op het gebruik maken van de gegevens die in de systemen staan. Het MID ziet juist wel op de goede werking van de systemen. De politie heeft daar verder dan ook geen rol in.

Vragenblok 22 - SP

De leden van de SP-fractie begrijpen dat achter het ESP ook de databases van Europol en Interpol zich bevinden. Kan de regering toelichten welke informatie in die databases op te vragen is?

Het ESP dient een aanvullend middel te zijn voor het doorzoeken van het centrale SIS, de Europol-gegevens en de Interpol-databanken. Dit ter aanvulling van de interfaces die daarvoor al beschikbaar zijn, zoals vastgelegd in de Interoperabiliteitsverordening politiële en justitiële samenwerking, asiel en migratie. Het staat alleen bevragingen toe indien gegevens worden gebruikt die gerelateerd zijn aan personen of reisdocumenten die in een Unie-informatiesysteem, in de Europol-gegevens of in de Interpol-databanken zijn opgenomen.

Met betrekking tot Europol gaat het om het bevragen van het Europol Informatiesysteem (EIS) via de bevragingsapplicatie QUEST. Deze database bevat onderzoeksinformatie uit alle EU-lidstaten over personen verdacht van of veroordeeld voor terroristische misdrijven en andere ernstige strafbare feiten die binnen het mandaat van Europol vallen.

Met de Interpol databases worden bedoeld de databanken voor gestolen en verloren reisdocumenten (SLTD-databank) en de databank voor reisdocumenten die voorkomen in uitgevaardigde Notices (TDAWN-databank). Met de beoogde EU-Interpol overeenkomst waar momenteel over onderhandeld wordt, worden de nodige garanties op het gebied van gegevensbescherming vastgelegd die het mogelijk maken dat het ESP verbinding maakt met de databanken van Interpol.

5. Uitvoeringsaspecten en gevolgen

5.1 Gevolgen voor de systemen

Vragenblok 23 - VVD

De leden van de VVD-fractie vragen hoe lang Nederland verwacht nodig te hebben om deze systemen te implementeren. Welke problemen worden er voorzien? Kan de regering daarnaast verder toelichten wat de functie en werking van het Europaloket zal zijn?

De vraag naar hoeveel tijd Nederland nodig heeft om deze systemen te implementeren kan niet los worden gezien van het feit dat de uitvoering van de verordening een complex traject is met veel onderlinge afhankelijkheden. Voor Nederland is, zoals ook in vragenblok 1 aan de orde kwam, essentieel dat kwalitatief hoogwaardige centrale Europese systemen tijdig beschikbaar komen, zodat er voldoende tijd is voor het nationale test- en implementatietraject. Dit geldt logischerwijze voor alle lidstaten. In Nederland is in 2018 dan ook besloten tot de opzet van een programma om de implementatie te begeleiden. Met de implementerende partners is binnen het programma besloten dat de Europese planning leidend is voor de Nederlandse implementatie. Nederland ligt voor de realisatie en implementatie op schema.

Daarbij zullen er uitdagingen op het gebied van capaciteit zijn en worden uitdagingen verwacht bij de grensposten bij de uitrol van de systemen, aangezien dat tot een piekbelasting zal leiden. Hiervoor zijn in Europa maatregelen voorzien om deze risico’s te mitigeren. Nederland heeft dan ook bij de Commissie aangegeven dat het belangrijkste punt voor de implementatie de beschikking over stabiele en kwalitatief hoogwaardige systemen op centraal niveau is. Daarnaast is er een afhankelijkheid van andere lidstaten, aangezien elk afzonderlijke systeem simultaan in alle lidstaten in werking zal treden. Wanneer één lidstaat niet gereed is, zal de inwerkingtreding worden uitgesteld. De Commissie heeft sinds juni 2020 een Rapid Alert proces opgezet waarmee de voortgang van de implementatie van de IT-systemen bij de lidstaten en het Europese agentschap Eu-LISA wordt gemonitord. Op basis van dat mechanisme kan snel gerichte ondersteuning worden geboden. Nederlandse experts zijn vertegenwoordigd in diverse Europese overleggen en expert groepen. Op deze wijze kan de vinger aan de pols worden gehouden over de voortgang en eventuele problemen.

Het beoogde tijdpad dat is gegeven met de financiering ziet in ieder geval op een periode tot ultimo 2027. Dan wordt verwacht dat alle verordeningen in werking zijn getreden en dat processen, techniek en personeel gestabiliseerd zijn.

Het Europaloket wordt gebouwd om ketenpartners te ontzorgen als een schakel tussen de nationale en Europese systemen. Daarbij levert het Europaloket verschillende diensten waarbij ketenpartners kunnen kiezen voor maatwerk op een manier die het beste aansluit op de voor hen toepasselijke situatie (bijvoorbeeld bevragen of muteren). De invoer in een Europees systeem vanuit een nationaal systeem kan via het Europaloket plaatsvinden. De gegevens die via het Europaloket uitgewisseld worden vallen uiteen in twee categorieën. Het betreft ofwel gegevensuitwisseling in het kader van grensverkeer en migratie van derdelanders ofwel bevraging van Europese databases met het oog op het voorkomen, opsporen of onderzoeken van terroristische misdrijven of andere ernstige strafbare feiten. De verantwoordelijkheid voor beide categorieën berichtuitwisseling via het Europaloket berust bij de minister van Justitie en veiligheid.

Vragenblok 24 - SP

De leden van de SP-fractie merken op dat met de logische onderverdeling van de verantwoordelijkheden bij verschillende overheidsdiensten en -organisaties het complex is om het overzicht te houden. De Europese Commissie is voor een deel verantwoordelijk. Tegelijk heeft eu-LISA een rol. Vervolgens zijn er in Nederland talloze organisaties bij betrokken. Wie is er eindverantwoordelijk voor de uitwisseling van alle gegevens?

De regering onderstreept het belang van goede waarborgen ten aanzien van de uitwisseling van deze gegevens. Ten aanzien van de Europese systemen geldt dat het beheer bij EU-Lisa ligt maar voor de verwerking van de verschillende gegevens in de systemen geldt dat er inderdaad meerdere bevoegde autoriteiten bij zijn betrokken. De Europese wetgever heeft dit punt herkend en erkend doordat geregeld is welke autoriteit verantwoordelijk is voor de gegevensverwerking, dan wel de lidstaten verplicht de verwerkingsverantwoordelijke aan te wijzen (zie in dit kader bijvoorbeeld artikel 57 van de Etias-verordening, artikel 39 van de EES-verordening en artikel 40 van de Interoperabiliteitsverordeningen). Op deze wijze is er altijd een organisatie verantwoordelijk voor de betreffende gegevens. Daarnaast geldt dat lidstaten verplicht zijn de Commissie en eu-LISA in kennis te stellen van zowel de bevoegde autoriteiten als verwerkingsverantwoordelijken, waarvan lijsten worden gepubliceerd. Uiteindelijk is Nederland als lidstaat verantwoordelijk voor de gegevensverwerking die niet door Europese instanties of een andere lidstaat wordt verricht.

5.2 Gevolgen voor uitvoerende organisaties

Vragenblok 25 - VVD

De leden van de VVD-fractie maken zich zorgen om de hoge werkdruk bij de IND, die met het toevoegen van deze extra taken alleen maar zal toenemen. De regering geeft aan dat er waarschijnlijk extra personeel zal moeten worden ingezet. Om hoe veel extra personeel (fte) gaat het en op welke termijn zal dit personeel geworven worden?

In overleg met ketenpartners is er voor gekozen om te voorzien in een gefaseerde opbouw van de personele bezetting. Hiervoor is gebruik gemaakt van een ingroeimodel. Wat wil zeggen dat het niet in de lijn der verwachting ligt dat al direct bij de start van de implementatie van de verordeningen het totaal aantal opgevoerde FTE’s door de ketenpartners nodig zal zijn en ook niet direct zal worden gerealiseerd. Daarnaast geldt dat de systemen die de verordeningen reguleren gefaseerd in gebruik worden genomen en daardoor de benodigde FTE ook gefaseerd beschikbaar kunnen komen. Momenteel is de verwachting, gebaseerd op de Europese planningen, dat in 2023 het aantal benodigde FTE 26 is, oplopend naar 46 in 2027.

Vragenblok 26 - SP

De leden van de SP-fractie lezen in de memorie van toelichting dat er bij de verschillende diensten en organisaties die met de systemen werken of gaan werken veel fte nodig is. Kan de regering schematisch weergeven waar precies hoeveel fte nodig is om de systemen te benutten? Hoe meent

de regering aan al die fte te komen in een tijd waarin meer vacatures zijn dan sollicitanten? En hoe voorkomt de regering dat deze nieuwe taken ten koste gaan van bestaande taken bij bijvoorbeeld de Koninklijke Marechaussee of de vreemdelingenpolitie?

Zoals tevens in reactie op de vragen van de leden van de VVD-fractie is weergegeven, is er in samenspraak met de verschillende ketenpartners voor gekozen om te voorzien in een gefaseerde opbouw van de personele bezetting. De systemen die worden gereguleerd door de verordeningen worden eveneens gefaseerd in gebruik genomen. Daarnaast geldt dat de werkzaamheden per systeem verschillen per ketenpartner. Daarbij kan sprake zijn van een intensieve rol in verband met een taak ten aanzien van registratie van gegevens in een systeem, of een beperkte rol doordat de betreffende ketenpartner alleen een systeem raadpleegt in specifieke gevallen. Ook geldt dat niet alle werkzaamheden en systemen nieuw zijn.

Ten aanzien van een schematische weergave van het aantal fte's dat nodig is bij alle ketenpartners om met de systemen te gaan werken geldt dat er door de ketenpartners voorlopige inschattingen zijn gemaakt. Het opnemen van een schematische weergave van het aantal benodigde fte's zou echter een beeld geven van harde vaststaande cijfers, terwijl zoals eerder aan bod kwam de Europese planning voor het in gebruik nemen van de systemen leidend is en alleen gewerkt kan worden met voorlopige inschattingen. Momenteel is de inschatting dat bij alle betrokken organisaties het aantal benodigde fte gedurende een aantal jaren zal oplopen naar ongeveer 360 fte.

Gezien de actuele situatie op de arbeidsmarkt, kan het een uitdaging zijn voor de individuele ketenpartners om de gewenste (nieuwe) medewerkers te werven. Om dit risico te mitigeren zijn er actieplannen die voorzien dat aanvullende wervingstrajecten binnen de ketenpartners worden opgestart om zo goed mogelijke de benodigde mensen aan te trekken. De ontstane vertragingen vanuit Europa ten aanzien van de inwerkingtreding van de verordeningen hebben hierbij ook een klein positief effect. De datum waarvoor de personele bezetting benodigd is wordt hiermee vooruit geschoven, de mogelijkheden voor de ketenpartners om de medewerkers tijdig te werven worden hiermee vergroot.

Nieuwe taken zullen niet ten koste gaan van bestaande taken omdat voor de uitvoering van de taken van de verordeningen specifiek is begroot en extra wordt geworven.

6. Gegevensbescherming en privacy-aspecten

6.1 Gevolgen voor de privacy

Vragenblok 27 - VVD

De leden van de VVD-fractie erkennen dat het implementeren van de verordeningen grote uitdagingen op het gebied van databescherming met zich meebrengt gezien de verwerking van persoonsgegevens. Op welke manier wordt gewaarborgd dat dit proces in alle lidstaten goed verloopt? Voldoen alle nationale systemen ook aan de minimale privacy-eisen?

Wat betreft het delen van gegevens tussen EU-lidstaten onderling vindt de regering dat de richtlijnen hier voldoende ruimte voor biedt, maar ook voldoende waarborgen bevat voor individuele personen (bijvoorbeeld als één van de EU-landen nauwe banden onderhoudt met een derde land van waaruit asielzoekers op de vlucht zijn), vragen de leden van de VVD-fractie.

Wat betreft het delen van gegevens met derde partijen vragen de leden van de VVD-fractie of de regering vindt dat de verordeningen een goede balans vinden in de ruimte voor het delen van gegevens (bijvoorbeeld met het oog op de nationale veiligheid) en privacyoverwegingen.

De bescherming van persoonsgegevens is op diverse niveaus in de verordeningen gewaarborgd. Voor wat betreft de veiligheid van de systemen zelf geldt dat de ontwikkeling en het beheer is

belegd bij het Europese agentschap eu-LISA. Deze systemen moeten aan hoge kwaliteitseisen voldoen, waaronder de bescherming van gegevens. Zo zijn er vanaf de ontwikkelfase al beveiligingsrisicobeoordelingen uitgevoerd en worden de beginselen van privacy door ontwerp en standaardinstellingen gevolgd. De lidstaten zijn verantwoordelijk voor de nationale systemen die worden aangesloten en dienen daartoe eveneens beveiligingsmaatregelen te treffen.

Voor wat betreft de bescherming van persoonsgegevens geldt daarnaast dat de verordeningen regelen dat de ter uitvoering van de verordeningen ingevoerde of opgevraagde gegevens niet voor andere doelen dan waarin de verordeningen voorzien worden verwerkt. Ook moeten de lidstaten ervoor zorgen dat verzamelde en opgeslagen gegevens rechtmatig worden verwerkt en alleen naar behoren gemachtigde personeelsleden toegang tot de systemen hebben voor de uitvoering van hun taken.

Vervolgens zijn in de verordeningen diverse controlemechanismen opgenomen. Naast het feit dat lidstaten aansprakelijk zijn voor schade geleden door onrechtmatige gegevensverwerking, geldt dat er logbestanden worden bijgehouden van het raadplegen van de systemen waaruit blijkt welke autoriteit met welk doel welke gegevens heeft geraadpleegd. Voor de personen van wie gegevens worden verwerkt geldt dat zij onder meer recht hebben op informatie, inzage en correctie van gegevens en er de mogelijkheid is om een klacht in te dienen bij de toezichthouder of een rechterlijke procedure te starten. Tot slot is er voorzien in toezicht op de verwerking van persoonsgegevens.

Alle voornoemde eisen en rechten gelden op grond van de verordeningen in alle lidstaten en op deze wijze wordt gewaarborgd dat de processen goed verlopen.

De verordeningen bevatten een goede balans tussen het kunnen delen van gegevens tussen de lidstaten en privacyoverwegingen. Het delen van gegevens is mogelijk indien daar een legitiem doel voor is zoals beschreven in de verordeningen, maar daarbij bevatten de verordeningen ook de randvoorwaarden en de eis van een beveiligde omgeving om dit te kunnen doen op een wijze die recht doet aan de privacybelangen van betrokkenen.

6.2 Rechten van betrokkenen en informatievoorziening

Vragenblok 28 - VVD

De leden van de VVD-fractie vragen op welke manier een betrokkene een beslissing kan aanvechten. Is hier een termijn aan verbonden? Zo ja, wat gebeurt er als deze termijn wordt overschreden?

Betrokkenen kunnen op grond van alle verordeningen beslissingen aanvechten en hun rechten uitoefenen. Als het gaat om bijvoorbeeld een besluit tot weigering van toegang, dan gelden daar de gebruikelijke bezwaar en beroepsmogelijkheden voor conform de Algemene wet bestuursrecht (Awb). Waar het gaat om het aanvechten van een beslissing op het terrein van privacybescherming geldt dat de verordeningen mede onder verwijzing naar de Algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging (RGB) bepalingen bevatten die ervoor zorgen dat de personen van wie persoonsgegevens worden verwerkt hun rechten kunnen uitoefenen. Zowel de EES-verordening, als de Etias-verordening, de herziening van de VIS-verordening, de SIS-verordeningen en de beide Verordeningen interoperabiliteit regelen dat betrokkenen hun verzoek tot bijvoorbeeld inzage of correctie van gegevens bij iedere lidstaat kunnen indienen. Ook de toepasselijke termijnen zijn geregeld. Daarbij dient de betrokkene te worden ingelicht over de wijze waarop hij een rechtsvordering kan instellen of een klacht kan indienen bij de bevoegde autoriteiten of bij de rechter in die lidstaat en over de bijstand die hem kan worden verleend door de toezichthoudende autoriteit (in Nederland dus de Autoriteit persoonsgegevens: AP). Indien de termijn wordt overschreden geldt de in de Awb opgenomen mogelijkheid van het opleggen van een dwangsom bij niet tijdig beslissen. Ook geldt dat indien een verplichting ten aanzien van gegevensverwerking niet wordt nagekomen, de betrokkene het recht heeft een klacht in te dienen bij de toezichthouder of een rechtsvordering in te stellen.

Vragenblok 29 - SP

De leden van de SP-fractie maken zich zorgen over het steeds makkelijker uitwisselen van gegevens tussen de landen in het Schengengebied. Foute registraties in het ene land kunnen gevolgen hebben in een ander land. Het is daarom belangrijk dat betrokkenen hun rechten uit kunnen oefenen. Kan de regering kort uitleggen waarom dit het geval is? Is het echt haalbaar voor personen in Nederland om inzicht te krijgen in informatie die door een ander land is ingevoerd en om die eventueel te wijzigen? Kan de regering ook iets meer toelichten over het in te richten centrale loket dat in de memorie van toelichting wordt aangekondigd?

Zoals ook toegelicht in de reactie op de vragen van de leden van de VVD-fractie (vragenblok 27) kennen de verordeningen specifieke bepalingen ten aanzien van de rechten van betrokkenen. De gegevens worden centraal opgeslagen in de Europese systemen waardoor er geen verschil in registraties kan ontstaan tussen de lidstaten. Ook het aanbrengen van interoperabiliteit tussen de verschillende systemen zorgt voor het voorkomen van verschillende registraties. Personen kunnen hun rechten uitoefenen in iedere lidstaat en daar een verzoek indienen tot bijvoorbeeld inzage of correctie van gegevens. Indien nodig wordt vervolgens door de lidstaat die het verzoek heeft ontvangen gevraagd aan de voor de verwerking verantwoordelijke lidstaat om de gegevens te controleren. Indien gegevens feitelijk onjuist zijn, onvolledig zijn of onrechtmatig zijn opgeslagen moeten deze worden gerectificeerd, aangevuld of verwijderd. Indien het verzoek wordt afgewezen of niet binnen de daarvoor in de verordening bepaalde termijn wordt gereageerd kan de betrokkenen een klacht indienen bij de toezichthouder of naar de rechter gaan, dan wel heeft de betrokkene recht op een dwangsom bij niet tijdig beslissen.

Nederland richt een centraal kantoor, ook wel ‘loket’ in voor de behandeling van AVG-verzoeken die betrekking hebben op de verwerking van persoonsgegevens door middel van de MID (‘multiple identity detector’ of detector van meerdere identiteiten), zodat betrokkenen effectiever gebruik kunnen maken van hun rechten met betrekking tot deze gegevensverwerkingen. De MID zorgt voor het aanmaken en opslaan van een identiteitsbevestigingsbestand, waarbij links tussen identiteitsgegevens in de verschillende Europese systemen kunnen worden aangebracht. Een persoon kan namelijk in meerdere systemen voorkomen. Ook ten aanzien van dit MID geldt dat personen het recht op toegang, rectificatie en wissing van gegevens hebben. Omdat deze gegevens gelinkt zijn met een van de onderliggende systemen geldt dat er verschillende bevoegde autoriteiten en verschillende lidstaten betrokken kunnen zijn bij een dergelijk verzoek. De lidstaten mogen op grond van de verordeningen beslissen dat antwoorden op dergelijke verzoeken gegeven worden door centrale kantoren. Omdat Nederland het belang onderkent voor burgers om hun rechten te kunnen uitoefenen wordt inderdaad gekozen voor het inrichten van een centraal kantoor zodat dit proces zo goed mogelijk verloopt.

Dit centrale kantoor voor de inzage en correctie van MID-gegevens wordt belegd bij de organisatie Justid, die ook de ketenprocescoördinatie op het aan de MID gerelateerde manuele verificatieproces doet. Justid verzorgt daarbij het ontvangen van de MID gerelateerde vraag en draagt in die hoedanigheid zorg voor het aan de betrokkene inzage geven in het door de betrokken ketenpartners gevolgde manuele verificatieproces. Justid verzorgt, indien dit aan de orde is, ook het doorgeleiden van vragen over in de MID vastgelegde identiteitsgegevens naar de bij de registratie betrokken verantwoordelijk autoriteiten. Met dit centrale kantoor wordt geborgd dat de burger één centraal aanspreekpunt heeft en houdt voor aan de MID gerelateerde inzage- & correctieverzoeken.

Vragenblok 30 - SP

In de reactie van de Autoriteit Persoonsgegevens is kritiek geuit op de hoogte van de boetes bij verwerking van gegevens in strijd met de verordeningen, zo lezen de leden van de SP-fractie. Kan de regering toelichten of zij tegemoet is gekomen aan die kritiek in de versie van de wet zoals die nu bij de Tweede Kamer ligt?

De verordeningen regelen dat de Algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging (RGB) van toepassing zijn, naast de

specifieke bepalingen die de verordeningen zelf bevatten. Voor de RGB geldt dat deze in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) is geïmplementeerd. Volgens de AP is er sprake van een discrepantie ten aanzien van de boete op doorgifte van gegevens aan derde landen in strijd met de verordeningen al naar gelang de vraag of dit onder de toepassing van de (U)AVG valt of de Wpg en Wjsg. Het advies van de AP is opgevolgd door specifiek voor de overtreding van de bepaling over de doorgifte van gegevens aan derde landen in het wetsvoorstel een bepaling op te nemen (artikel 9) die voorziet in gelijke maximumboetes, ongeacht of de verwerking van persoonsgegevens wordt beheerst door de (U)AVG of de Wpg en Wjsg.

6.3 Rechtsmiddelen gegevensbescherming

Vragenblok 31- VVD

De leden van de VVD-fractie vragen op welke manier niet-Nederlanders aanspraak kunnen maken bij de AP. Kunnen mensen zonder verblijfsvergunning dit ook al doen?

De verordeningen kennen rechten op het terrein van de verwerking van persoonsgegevens toe aan de personen van wie gegevens in de systemen worden verwerkt. Dit zijn bij uitstek onderdanen van derde landen zonder verblijfsvergunning nu het bijvoorbeeld gaat om inreis en uitreis voor kort verblijf Schengen (EES), een reisautorisatie voor kort verblijf (Etias) of een visum voor onderdanen van derde landen (VIS). Hetzelfde geldt voor signaleringen ten aanzien van een terugkeerbesluit, een inreisverbod of een ongewenstverklaring (SIS). Alleen ten aanzien van signaleringen op het terrein van politiële en justitiële samenwerking kunnen ook Unieburgers worden geraakt.

De toezichthoudende autoriteiten van de lidstaten hebben op grond van de verordeningen taken gekregen op het terrein van bijstand en ondersteuning. Dit geldt dus ook voor de Autoriteit Persoonsgegevens.

De Autoriteit Persoonsgegevens heeft desgevraagd aangegeven dat de wijze waarop niet-Nederlanders hun rechten kunnen uitoefenen met betrekking tot het Schengen Informatiesysteem II (SIS II) en het Visum Informatiesysteem (VIS) wordt toegelicht op de website van de AP. Ook mensen zonder verblijfsvergunning kunnen dit doen.

In de toekomst zal dit dus ook voor de nieuwe systemen gaan gelden. Daarnaast geldt dat personen op verschillende andere manieren worden gewezen op hun rechten. Bij afgifte of weigering van een reisautorisatie wordt bijvoorbeeld tevens informatie verstrekt over de rechten en procedures ten aanzien van de bescherming van persoonsgegevens.

7. Consultatie paragraaf

Vragenblok 32 – D66

De leden van de D66-fractie vragen of de regering nader kan onderbouwen waarom niet is gekozen de rechter-commissaris aan te wijzen als centraal toegangspunt dat toegang geeft tot de Europese informatiesystemen, zoals de AP aanbeveelt.

De EES-verordening, de Etias-verordening, de VIS-verordening, maar ook de Eurodac-verordening geven bepaalde materiële en procedurele voorwaarden voor het raadplegen van het desbetreffende informatiesysteem met het oog op de opsporing en vervolging van strafbare feiten. Het centraal toegangspunt heeft tot taak het verifiëren of aan alle voorwaarden is voldaan.

De regering staat voor dat de officier van justitie fungeert als centraal toegangspunt en niet de rechter-commissaris. Hiervoor is het volgende van belang. De attributie van strafvorderlijke bevoegdheden vindt plaats op basis van de ingrijpendheid van de bevoegdheden – de inbreuk die toepassing van de bevoegdheid maakt op de rechten van de betrokkene. Naargelang de mate van ingrijpendheid van de bevoegdheid toeneemt, dient de uitoefening te worden voorbehouden aan een qua waarborgen voor kwaliteit, onafhankelijkheid en onpartijdigheid beter toegerust orgaan. Hier hangt mee samen dat bevoegdheden van vergelijkbare mate van ingrijpendheid zijn

geattribueerd aan hetzelfde orgaan. Gelet op de mate van ingrijpendheid van het raadplegen van de desbetreffende informatiesystemen alsmede gelet op de verhouding tot andere strafvorderlijke bevoegdheden meent de regering dat de officier van justitie als centraal toegangspunt passend is.

In reactie op het advies van de Autoriteit Persoonsgegevens is opgemerkt dat de verordeningen niet vereisen dat de taak van centraal toegangspunt bij een rechter wordt belegd, maar slechts vereisen dat de als centraal toegangspunt aangewezen autoriteit onafhankelijk is ten opzichte van de autoriteiten waaraan toegang kan worden verleend tot de desbetreffende informatiesystemen. Dit is met de officier van justitie als centraal toegangspunt het geval. Conform het advies van de Raad van State bij het wetsvoorstel is in artikel 4, tweede lid, van het wetsvoorstel expliciet vastgelegd dat bij de uitoefening van de taken en bevoegdheden, bedoeld in het eerste lid, de officier van justitie volledig onafhankelijk optreedt ten opzichte van de in artikel 3 aangewezen autoriteiten, alsmede van de officier van justitie die het gezag over die autoriteiten uitoefent.

Vragenblok 33 – D66

Daarnaast vragen de leden van de D66-fractie of de regering nader kan onderbouwen waarom er (naast een invoeringstoets) geen evaluatiebepaling is opgenomen, zoals de AP aanbeveelt.

Voor wat betreft het opnemen van een evaluatiebepaling geldt dat een zelfstandige evaluatie van de voorgestelde uitvoeringswet niet noodzakelijk is gelet op de verschillende algemene evaluatiebepalingen die al in de verordeningen zelf zijn opgenomen. Op grond van deze bepalingen wordt de werking van de verordeningen waaronder de toepassing van de betreffende verordening in de praktijk geëvalueerd en zijn de lidstaten verplicht de daarvoor benodigde informatie aan te leveren. Gelet op het feit dat het wetsvoorstel dient ter uitvoering van de betreffende EU-verordeningen, ligt het voor de hand deze Europese evaluaties te volgen en indien nodig vervolgens het wetsvoorstel aan te passen en niet het wetsvoorstel zelf te evalueren los van de werking van de verordeningen.

Ten aanzien van het uitvoeren van een invoeringstoets geldt dat voor de uitvoering van een dergelijke toets geen wettelijke bepaling vereist is. Om die reden zal na de inwerkingtreding van het wetsvoorstel het geldende kabinetsbeleid ten aanzien van het uitvoering van een invoeringstoets dan ook gevolgd worden.

Vragenblok 34 - SP

De leden van de SP-fractie willen markeren dat het wetsvoorstel een forse impact heeft. Tegelijk volgt deze wetgeving uit Europese verordeningen. Toch menen deze leden dat er meer aandacht nodig is voor dit voorstel. Waarom heeft de regering de organisaties die moeten gaan werken met deze gegevensbanken niet om een publieke reactie gevraagd? En waarom zijn er geen niet-gouvernementele organisaties die actief zijn op het terrein van gegevensbescherming benaderd voor input? De consultaties die nu meegezonden zijn met het voorstel zijn in de ogen van deze leden wel erg beperkt gezien de reikwijdte van het voorstel.

De organisaties die gaan werken met de verschillende systemen zijn niet om een publieke reactie gevraagd omdat zij deelnemen in het voor de uitvoering van de verordeningen opgezette programma grenzen en veiligheid. Waar de consultatie van een wetsvoorstel een momentopname betreft van de standpunten van de betreffende organisaties, wordt met het programma op doorlopende wijze de betrokkenheid van deze organisaties gewaarborgd. Daarnaast geldt dat de verplichtingen die in de verordeningen zijn opgenomen waaronder waarborgen op het terrein van gegevensbescherming al vastliggen en niet meer gewijzigd kunnen worden. Op Europees niveau worden voorstellen voor Europese regelgeving geconsulteerd, waarop een ieder kan reageren.

Vragenblok 35 - SP

Het is de leden van de SP-fractie opgevallen dat de Raad voor de Rechtspraak (Rvdr) in haar advies zich beperkt tot de totstandkoming van Etias terwijl het voorstel veel meer behelst. Heeft de RvdR aangegeven waarom ze deze beperking aanbrengt?

De Raad voor de Rechtspraak heeft opgemerkt geen aanleiding te zien tot het maken van inhoudelijke opmerkingen maar wel gevolgen te zien voor de werklast van de Rechtspraak, met name de bestuursrechtspraak. De Raad heeft niet aangegeven waarom deze beperking is aangebracht. Dat neemt niet weg dat het voor de hand ligt dat de Raad naar de gevolgen voor de werklast heeft gekeken van Etias, omdat op grond van de Etias-verordening in combinatie met de voorgestelde Uitvoeringswet een nieuwe taak wordt ingevoerd op grond waarvan besluiten tot afgifte of weigering van een reisautorisatie worden genomen. Tegen deze besluiten staat bezwaar en beroep open. Het instellen van beroep heeft gevolgen voor de werkbelasting van de gerechten. Bij de andere verordeningen speelt dat niet op deze wijze omdat er daar sprake is van bestaande besluitvorming en rechtsbescherming. Dit is tevens beschreven in de memorie van toelichting in de paragraaf over de gevolgen voor de rechtspraak.

De Staatssecretaris van Justitie en Veiligheid,