Panteia
Research to Progress

Research voor Beleid | EIM | NEA | IOO | Stratus | IPM

Gebruik van passagiersgegevens voor grenscontrole

Evaluatie van de uitvoering van de API-richtlijn

Auteurs:
Guido Brummelkamp
René Vogels

Zoetermeer, 11 december 2018

Inhoudsopgave

Samenvatting

Achtergrond onderzoek
Ten behoeve van het verbeteren van de grenscontroles en het tegengaan van illegale migratie zijn luchtvaartmaatschappijen verplicht om bepaalde gegevens van alle passagiers en bemanningsleden die van buiten het Schengengebied en van buiten de Europese Unie naar Nederland vliegen, te verstrekken aan de autoriteiten die belast zijn met grenscontrole. Deze gegevens verstrekken zij aan de Koninklijke Marechaussee (KMar). In Nederland is de KMar de met de grenscontrole belaste autoriteit. De gegevens die de KMar krijgt komen uit het reisdocument en worden aangevuld met enkele gegevens over de vlucht en de boeking. Deze gegevens staan bekend als Advance Passenger Information (API). Advance verwijst naar het moment waarop de gegevens moeten worden verstrekt: namelijk aan het einde van de instapcontroles en daarmee ruim voordat de passagiers aankomen op de bestemming. Nederland heeft met deze verplichting de Europese Richtlijn 2004/82/EG geïmplementeerd. De verplichting is opgenomen in de Vreemdelingenwet 2000.

Met dit onderzoek is het gebruik van API-gegevens in Nederland geëvalueerd. Het onderzoek is een vervolg op de eerste evaluatie van API in 2014. Op grond van dit eerste evaluatieonderzoek heeft de minister van Justitie en Veiligheid de Tweede Kamer toegezegd een tweede evaluatiestudie te laten uitvoeren als onder andere het systeem verder is uitontwikkeld.

Voor deze tweede evaluatie zijn twee centrale onderzoeksvragen geformuleerd:
- Wat kan gezegd worden over het gebruik en de effectiviteit van API-gegevens ten behoeve van grenscontrole en het tegengaan van illegale immigratie en op welke wijze is gevolg gegeven aan eerdere aanbevelingen ten aanzien van API?
- In hoeverre kunnen recente relevante Europese ontwikkelingen gevolgen hebben voor de wijze waarop API-gegevens in Nederland gebruikt worden?

Voor dit onderzoek zijn interviews gehouden met:
- vertegenwoordigers van drie Nederlandse luchtvaartmaatschappijen en de internationale belangenorganisatie voor de luchtvaart (IATA),
- medewerkers van de KMar,
- medewerkers bij de ministeries van Justitie & Veiligheid, Infrastructuur & Waterstaat en Defensie,
- een wetenschappelijk onderzoeker op het gebied van passagiersinformatie.

Daarnaast zijn schriftelijke bronnen geraadpleegd. Voor de kwantitatieve analyses is gebruikgemaakt van tellingen per maand over de periode november 2013 tot en met maart 2018. De tellingen hebben we via de KMar ontvangen. Deze tellingen zijn niet over de gehele periode volledig en niet vergelijkbaar over de gehele periode vanwege wijzigingen door de jaren in het aantal luchthavens waarvoor de API-verplichting van

kracht was. Om een beeld te krijgen van de werking van API in de praktijk is op twee ochtenden meegelopen met de KMar op de werkvloer. Op basis daarvan zijn enkele casussen beschreven die in deze rapportage zijn opgenomen.

Gebruik van API-gegevens

Voor het beantwoorden van de eerste onderzoekvraag is allereerst beschreven hoe API-gegevens volgens de API-richtlijn precies verondersteld worden bij te dragen aan een het verbeteren van de grenscontrole en aan het tegengaan van illegale migratie. Door al bij vertrek van een vlucht naar Nederland over passagiersgegevens te beschikken, kan de KMar voorwerk doen. De KMar kan aan de hand van de API-gegevens tijdens de vlucht beoordelen of er mensen aan boord zitten die voorkomen in verschillende opsporingsregisters, watchlists of mensen die vanwege een combinatie van persoons- en vluchtgegevens matchen met een profiel. Een profiel kan zijn gebaseerd op verschillende variabelen. Bijvoorbeeld de combinatie van omvang reisgezelschap, land van vertrek, nationaliteit, leeftijd en sexe.

Deze 'screening' wordt gedaan door het API-Centrum, een onderdeel van het Targeting Center Borders. De Sectie Analyse & Onderzoek (Sectie A&O) draagt bij aan het screeningsproces met de ontwikkeling van profielen. Het screeningsproces levert in eerste instantie zogenaamde 'matches' op: de API-gegevens komen in die gevallen overeen met een opsporingsdatabase, watchlist of profiel. Deze matches worden vervolgens gevalideerd en worden dan als het blijkt te gaan om een passagier die bij de grens of de gate nadere aandacht behoeft een 'hit' genoemd. Bij een hit zijn onder andere de persoonsgegevens gecontroleerd en is beoordeeld of de signalering nog actueel is. In deze fase kan aanvullende informatie worden toegevoegd. Hierbij kan het gaan om bijvoorbeeld een foto of voorgestelde manier van bejegening. Indien het API-Centrum constateert dat er sprake is van een hit, verstuurt zij aan de operatie een opdracht ter uitvoering van een interventie. Deze opdrachten worden alerts genoemd en kunnen verschillende acties omvatten. Voor het acteren op alerts beschikt de KMar, naast de reguliere grenscontrole, over onder andere een mobiel team van Dedicated Gate Control (DGC). DGC kan passagiers waarvoor een alert is uitgegaan al bij het verlaten van het vliegtuig aan de gate opwachten. De KMar kan op basis van de API-gegevens en de analyses gericht optreden.

Het aantal alerts is in de afgelopen jaren gestaag toegenomen van zo'n 200 per maand in 2013 naar circa 1.200 per maand in de eerste drie maanden van 2018. Deze trend volgt de groei van het grensverkeer met betrekking tot vluchten waarvoor de API-verplichtingen gelden. De stijging hangt verder samen met het feit dat vanaf 1 juni 2016 voor alle luchthavens van buiten het Schengengebied de API-gegevens moeten worden aangeleverd. Eind 2013 was de verplichting beperkt tot 54 luchthavens. Het aantal alerts betreft ongeveer 0,1% van het totaal aantal passagiers dat van buiten Schengen in Nederland aankomt. Per maand verschilt het percentage binnen een kleine bandbreedte. In de eerste drie maanden van 2018 is het iets gestegen tot net boven de

0,1%. In 2017 en het eerste kwartaal van 2018 gaat het om gemiddeld ruim 1 miljoen passagiers per maand die via een luchthaven in Nederland aankomen waarvoor de API-verplichtingen gelden.

Effectiviteit API

Het aantal alerts dat betrekking heeft op (een risico op) illegale immigratie komt uit op 421 passagiers in 2017 (3,6% van alle alerts in dat jaar). In ongeveer 120 gevallen is in 2017 op basis van een alert aantoonbaar met de verwerkte terugkoppeling in de database een persoon de toegang tot Nederland (Schengen) geweigerd. Ongeveer 14% van de alerts heeft betrekking op passagiers van wie het reisdocument als vermist of gestolen staat geregistreerd.

Een groot deel van de alerts (38%) betreft passagiers die gesignaleerd staan vanwege een zogeheten Mulderfeit (verkeersboetes). Het gaat om passagiers die na herhaalde betaalverzoeken nog steeds één of meerdere verkeersboetes niet hebben betaald.

De medewerkers van de KMar die dagelijks betrokken zijn bij grenscontrole benadrukken de meerwaarde van API. Zij geven aan dat API-gegevens bijdragen aan een effectievere grenscontrole.

Die meerwaarde is drieledig:

- In de eerste plaats is er meer tijd om passagiersgegevens te vergelijken met databases, watchlisten en profielen. De gegevens zijn immers beschikbaar op het moment dat het vliegtuig is vertrokken. Ook is er meer gelegenheid om een hit te toetsen bij een collega. KMar hanteert namelijk het vierogenprincipe. Er is altijd een tweede persoon die meebeoordeelt. Bij een alert met een hoge urgentie kan het mobiele team van DGC worden ingeseind om de betreffende passagier bij de gate op te wachten. De KMar kan dankzij API de capaciteit gericht inzetten.
- In de tweede plaats kan het API centrum bijzonderheden en risico's signaleren die bij een grensdoorlaatpost buiten beeld blijven. Het API-Centrum kan bijvoorbeeld zien of een passagier via een ongebruikelijke route reist, of dat de passagier onderdeel is van een opvallend reisgezelschap. Dit soort afwijkingen kan een indicatie zijn van een verhoogd risico op illegale migratie en daarmee reden om bij aankomst in Nederland gericht vragen te stellen.
- In de derde plaats omdat het de controle bij de grensprocessen verbetert en versnelt omdat vooraf de passagiersgegevens beschikbaar en geanalyseerd zijn. De controle aan de doorlaatposten beperkt zich tot identificatie van de passagier en de geldigheid van diens reisdocument. Dit verbetert de doorstroming van reizigers en voorkomt wachtrijen aan de grensdoorlaatposten. Voor luchtvaartmaatschappijen en passagiers is dit een belangrijke meerwaarde. Zonder API zou de KMar van alle passagiers immers pas op het moment van aankomst de vergelijking met opsporingsregisters en watchlists kunnen uitvoeren.

De onderzoekers plaatsen drie belangrijke kanttekeningen bij het gebruik van API-gegevens.

- Alerts worden handmatig doorgegeven aan de grensdoorlaatposten. De doorgegeven alerts worden door de groepscommandanten van de grensdoorlaatposten uitgeprint, zij zorgen er vervolgens voor dat deze prints op de desks van de grenswachter(s) komen te liggen. Deze werkwijze doet een beroep op de oplettendheid van de grenswachten. Van hen wordt verwacht dat zij de op papier aangeleverde alerts tot zich nemen en onthouden om zo de betreffende passagiers ook daadwerkelijk te herkennen op het moment dat zij de grens willen passeren. Volgens betrokken KMar-medewerkers zijn de grenswachten voldoende oplettend. Het is echter voor de onderzoekers niet te bepalen of dat daadwerkelijk zo is en hoe vaak het voorkomt dat een gesignaleerde passagier desondanks niet wordt aangehouden.
- API-gegevens bieden meer mogelijkheden om passagiers te detecteren dan alleen via de vergelijking met databases. Bijvoorbeeld passagiers die niet staan gesignaleerd in een database/opsporings-systeem maar toch nadere aandacht behoeven. Het betreft met name de detectie van 'unknown persons with an unknown risk', die op basis van de combinatie persoons- en reisgegevens uit de passagiersstroom gefilterd kunnen worden. Dit proces vindt nu nog vooral handmatig plaats. Er worden stappen gezet om hierbij meer gebruik te maken van automatisering. Bijvoorbeeld door gebruik van algoritmes waarmee systematisch gezocht kan worden naar afwijkende patronen en afwijkingen van het normbeeld.
- De derde kanttekening heeft betrekking op het begrip bij luchtvaartmaatschappijen, maar ook bij anderen die met deze gegevens en verplichtingen te maken hebben, voor de strikte juridische scheiding tussen de huidige API-verplichtingen en het gebruik van passagiersgegevens door de Douane en het PNR-wetsvoorstel. In het PNR-wetsvoorstel is voorzien dat luchtvaartmaatschappijen Passenger Name Record (PNR) gegevens aanleveren. PNR-gegevens bevatten informatie die luchtvaartmaatschappijen nodig hebben om reserveringen te kunnen verwerken en te controleren. Naast persoonsgegevens als naam, geboortedatum, gaat het om bijvoorbeeld betalingsgegevens, reisgenoten, bagage, en plaats in het vliegtuig. Het PNR-wetsvoorstel is op 9 januari 2018 aan de Tweede Kamer aangeboden. Indien het voorstel wordt aangenomen moeten luchtvaartmaatschappijen voor iedere passagier op verschillende momenten gegevens aanleveren bij twee verschillende loketten: één keer bij het API-Centrum op dezelfde wijze als tot nu toe en drie keer bij Pi-NL. Pi-NL is 'single window' voor passagiersinformatie in Nederland. Bij Pi-NL moeten zowel de PNR-gegevens als de API-gegevens worden aangeleverd.

De verplichting voor luchtvaartmaatschappijen om naast API ook PNR gegevens (nu alleen aan de Douane, en op termijn ook op basis van de PNR-wet) aan de overheid te verstrekken roept vragen op bij luchtvaartmaatschappijen ten aanzien van efficiëntie en effectiviteit. De praktijk in de bijvoorbeeld de VS en de Golfstaten is al dat wordt gewerkt met één loket. Luchtvaartmaatschappijen in Nederland maar ook de brancheorganisatie IATA pleiten voor een 'single window'. Als de PNR-wet is aangenomen verzamelt Nederland via twee kanalen passagiersgegevens. Voor luchtvaartmaatschappijen is dit een extra administratieve belasting. De Nederlandse overheid heeft dit probleem onderkend en onderzoekt de mogelijkheden om de aanlevering van de gegevens via een 'single window' mogelijk te maken.

Gevolgen van Europese ontwikkelingen

Op Europees niveau wordt gewerkt aan een breed pakket van maatregelen om de buitengrenzen te versterken. API was de eerste bouwsteen. De combinatie van meer passagiers en hogere veiligheidseisen zijn aanleiding geweest om te zoeken naar mogelijkheden om grote passagiersstromen zonder opstoppingen te kunnen afhandelen en daarbij geen concessies te doen aan veiligheidseisen en het respect voor de rechten van passagiers. De verwachting is dat de groei van passagiersstromen van buiten Schengen en de EU de komende jaren doorzet (van de circa 50 miljoen niet-EU passagiers in 2015 naar 76 miljoen in 2025).

Belangrijke recente ontwikkelingen en maatregelen worden gebundeld onder de noemer Smart Borders. Het gaat hierbij om o.a.:

- Entry-Exit System (EES): in november 2017 heeft de Europese Raad bepaald dat er een EES komt. Hiermee worden alle Schengengrensoverschrijdingen van niet-EU ingezetenen geregistreerd.
- European Travel Information and Authorization System (ETIAS): de Europese Raad heeft 5 september 2018 een verordening aangenomen die bepaalt dat er een Europees systeem voor reisinformatie en -autorisatie wordt opgezet. Het systeem is vergelijkbaar met het Amerikaanse Electronic System for Travel Authorization (ESTA). Het houdt in dat niet-visumplichtige onderdanen van derde landen voor hun reis naar een Schengenland een reisautorisatie moeten aanvragen.
- Systematische grenscontrole aan de hand van databases: op 7 maart 2017 heeft de Europese Raad een verordening tot wijziging van de Schengengrenscode aangenomen om de controles aan de buitengrenzen aan te scherpen. De lidstaten zullen alle mensen aan de grenzen systematisch moeten controleren aan de hand van relevante databanken.
- Interoperabiliteit: binnen de EU wordt gewerkt aan de verbetering van interoperabiliteit van informatiesystemen, zoals o.a. EES, Visa Information System (VIS), ETIAS en Schengen Information System (SISII). De bedoeling is dat deze systemen beter op elkaar aansluiten en elkaars gegevens kunnen gebruiken.
- Verbetering van SISII: er worden onder andere nieuwe categorieën van signaleringen aan SISII toegevoegd.

Bij invoering van EES en ETIAS is het mede in het kader van de carrier liability van belang dat luchtvaartmaatschappijen kunnen beoordelen of de 90 dagen termijn niet is overschreden en of iemand een ETIAS reisautorisatie heeft. Een verblijf van maximaal 90 dagen is namelijk toegestaan voor niet-visumplichtige derdelanders. Carrier liability duidt op het verantwoordelijk kunnen maken van de luchtvaartmaatschappij voor het verzorgen van de terugreis als iemand niet kan worden toegelaten tot Nederland.

API gegevens worden op dit moment niet gebruikt bij uitreizen. Als dat wel het geval is zijn niet-EU-passagiers effectief te signaleren die te lang binnen de EU-grenzen zijn gebleven. Langer dan op basis van de regelgeving mag. Toegestaan is een kort verblijf van maximaal 90 dagen. Nu kunnen die reizigers alleen worden gesignaleerd door de analyse van de datumstempels in paspoorten en dat kost relatief veel tijd en is foutgevoelig. API gebruiken bij uitreizen maakt het ook

mogelijk passagiers die voorkomen uit de registers (OPS, SIS) te signaleren.

Vergelijkbare systemen om voor het vertrek aan te geven of passagiers toestemming hebben af te reizen naar het bestemmingsland zijn al in werking in de VS, Canada en Australië. Deze landen vallen buiten de reikwijdte van de Europese API richtlijn maar geven mogelijk een richting aan voor de vorm die de EU-lidstaten kunnen kiezen met betrekking tot de combinatie van gegevens en registers om de toegang van passagiers te beoordelen. Luchtvaartmaatschappijen krijgen hierbij voorafgaand aan het boarden per passagier een OK/NOT OK TO BOARD signaal. Daarmee is meteen duidelijk of iemand mag afreizen naar het land van bestemming en lopen de luchtvaartmaatschappijen geen risico dat zij aansprakelijk worden gesteld voor het betalen van de terugreis. Bovendien kan dit een bijdrage leveren aan het verhogen van de veiligheid aan boord omdat op basis van opsporingsdatabase of watchlist potentieel gevaarlijke personen niet aan boord worden toegelaten.

De verwachting, en zeker bij de luchtvaartmaatschappijen ook de wens, is dat op de langere termijn 1 loket 'a single window' voor het aanleveren van passagiersgegevens een wereldwijd toegepast model wordt. In verschillende landen is dat nu al het geval. De API-verplichtingen zijn nu in Nederland opgenomen in de Vreemdelingenwet en gelden ook voor Nederlandse passagiers. Naast de stroom API-passagiersgegevens krijgt een andere autoriteit in Nederland nu al de PNR-gegevens, namelijk de Douane. Als de PNR-wet wordt aangenomen mogen aangewezen Bevoegde Instanties de PNR gegevens vorderen bij Pi-NL om te gebruiken voor het bestrijden van ernstige criminaliteit en terrorisme. De verschillende autoriteiten doen vervolgens vergelijkbare screenings en analyses op basis van deze bestanden. Ze gebruiken allemaal (delen van) registers als OPS, SIS en de watchlist. Het inbedden van de API- en PNR-verplichtingen in één kaderwet die ziet op passagiersgegevens is in onze ogen een logische route voor de toekomst. Dit zou zeker helpen om de transparantie bij alle partijen te verhogen.

Summary

Study background

In order to improve border controls and prevent illegal immigration airline companies are obliged to provide the authorities responsible for border control with certain personal details from passengers and cabin crew arriving from outside the Schengen and European Union area. In the Netherlands, the body responsible for guarding national borders is the Royal Netherlands Marechausee, henceforth referred to as KMar. The KMar receives personal details from an individual's travel document, and these details are supplemented by certain details concerning the flight and the booking process. These details are known as Advance Passenger Information (API). In this context, 'advance' refers to the moment at which these details must be provided, namely, at the end of the boarding process. By adopting this approach to the provision of personal details, the Netherlands implements and adheres to the requirement in the European Directive on the obligation of carriers to communicate passenger data (Directive 2004/82/EG). The requirement concerning personal information has been transposed into the Dutch Vreemdelingenwet 2000 (Alien act).

This current study evaluates the use of API-data in the Netherlands. The research is a follow-up study to the evaluation of API conducted in 2014. At that time, the API-system was still being developed. Based on the first evaluation study of the system, the Minister promised the Dutch national parliament that a second evaluation study would be conducted once the system was fully developed.

For this second evaluation study, two main research questions have been formulated:

- What can be said regarding the use and the effectiveness of API-details in aid of border controls and the prevention of illegal immigrants, and in which way have earlier recommendations regarding the API been considered?
- To what extent can recent relevant European developments have an impact on the way in which the Netherlands uses API data?

As part of this study, a literature review phase has been conducted, along with a series of interviews with:

- representatives from three Dutch airlines and the international sector organisation for air transport (the IATA),
- employees from KMar.
- policy makers from relevant ministries,
- and a scientific researcher.

The study also entailed a quantitative component, which involved examining counts per month for the period of November 2013 to March of 2018. These counts were not available for the entire period, nor are they comparable for that period. The reason for this being that there have been changes in the number of airports where the API requirement was in place. To gain an accurate impression of the way in which API works in practice, members of the research team joined KMar employees

on the work floor. Based on the two mornings during which the researchers joined the KMar, several cases have been developed and included in the report for this study.

Use of API details

In order to answer the first research question, the study first describes how exactly API details are expected to contribute to more effective border controls and the prevention of illegal immigration. The KMar obtains the passenger data following the controls and inspections that take place in the boarding process when taking a flight to the Netherlands. Airline companies collect and check the data and send these to the KMar when the flight has departed. API data are based on passport information and contain supplementary details about the flight and the booking itself.

Based on the API data, the KMar can evaluate the individuals on board the flight by checking whether any of the individuals appear in any of the various international and national detection databases, or on watchlists or match with a profile based on their personal and flight details. A risk profile can be based on different variables. For example, the combination of the size of the travelling party, the country of departure, nationality, age, and gender can all play a role.

The screening involved in this evaluation process is carried out by the API Centre, a component of the Target Centre Borders. The department A&O (Analysis & Research) contributes to the screening process by, for instance, providing the API centre with profiles. The screening process leads to so-called 'matches'. In those situations, the API data match with a detection database or profiles. These matches are then examined in further detail and validated, and are then referred to as a 'hit' if the passenger requires additional attention at the gate or at the border. Any given hit involves, among other things, the checking of personal details, and establishing whether the detection is still relevant. During this phase, additional details can be linked to the hit. The additional details may take various forms, such as a photograph, or an anticipated approach to treating the case. In situations where the API Centre establishes that a hit has indeed been identified, it then sends instructions to the operational organisation that an intervention must take place. These instructions are referred to as alerts, and can involve different types of action. In order to respond to alerts, the KMar houses a mobile team for Dedicated Gate Control (DGC) alongside its regular border control branch. The DGC can then await and intercept passengers for whom an alert has been made at the airport gate. Thus, the KMar can take action in a timely fashion due to the API data and the analysis of those data.

The number of alerts has steadily increased in recent years from some 200 alerts a month in 2013, to more than 1,100 alerts a month during the first three months of 2018. This trend follows the general increase in border traffic relating to flights were API requirements apply, and the fact that from the 1st of June 2016 onwards, all airports outside of the Schengen zone needed to provide API data. Before that time, the requirement of delivering API data was limited to 54 airports. The

number of alerts is equal to around 0.1% of the total number of passengers that enter the Netherlands form outside the Schengen area. The percentage differs slightly from month to month. During the first three months of 2018, this proportion increased slightly to just over 0.1%. The total number of passengers differs per month as well; in 2017 and during the first quarter of 2018, there were on average some 1 million passengers per month.

Effectiveness of API

The number of alerts which relate to (the risk of) illegal immigration was around 421 passengers in 2017 (which is equivalent to 3.6% of all alerts in that year). In 2017, there were around 120 instances where an alert and the connected database analyses have led to a person being denied entry to the Netherlands (Schengen). Around 14% of the alerts applies to passengers whose travel document has been lost of is registered as stolen.

A large part of all alerts (38%) concern passengers who have been detected because they have so-called 'Mulderfeiten' (traffic fines in The Netherlands) on their personal dossier that have not (yet) been resolved. For example, if a passenger has one or more unpaid traffic tickets, despite several requests for payment, they may be detected.

The KMar employees who are involved with border controls on a daily basis emphasise the worth and utility of API. They indicate that the API details contribute to more effective border control.

The added value of the API details are threefold:

- First of all, there is more time to compare passenger data based on databases and risk indicators as the data are available from the moment that the airplane departs. Furthermore, there is more time and opportunity to consult colleagues regarding a hit. KMar follows a four-eye principle; there is always a second individual who assess a hit. In cases concerning an alert with high urgency, the DGC's mobile team can be informed in order to intercept the passenger in question at the gate.
- Secondly, the API centre can report irregularities and risks that are not examined at a border post. The API centre has broader insight in this respect. The API centre can, for instance, see if a passenger travels using an irregular route, or whether a passenger is accompanied by surprising or unusual travellers. These sorts of irregularities can be an indication of a heightened risk of illegal immigration, and can constitute a reason for asking the passenger pointed questions when they arrive in the Netherlands.
- Thirdly, the API data provide added value as the control procedures at the borders are improved and made quicker as passenger details are available for examination beforehand. The controls and the entry points can be used only for the identification of passengers and the validity of their travel document. This improves the flow of travellers and prevents long lines and waiting at the entry points, and this is an important added value for airlines and passengers. Without API, the KMar would have to compare the details of all passengers to detection databases and lists at and after the arrival of passengers in the Netherlands.

The researchers identify three important considerations in the use of API details.

- Alerts are transferred manually to the enter points. The alerts are printed out by the group commanders for the entry points, and these group commanders ensure that the printouts of the alerts arrive at the desks of the border guards at the entry points. This way of working is relatively demanding in that it relies strongly on the attentiveness and alertness of the border guards. These individuals are expected to receive the printed information regarding the alerts, to understand and retain the information, and to actually recognise the passengers concerned when they try to cross the border. According to KMar employees involved with this process, the border guards are sufficiently alert and attentive. However, it goes beyond the scope of this research to establish to what extent that is indeed the case, or to establish how often passengers for whom alerts have been disseminated, are not intercepted in practice.
- API details offer more possibilities to detect passengers beyond purely comparing their details with detection databases. Passengers who have not been detected or signalled in a database or detection system may still warrant further attention. This issue applies mainly to the detection of 'unknown persons with an unknown risk', who can be filtered out of the flow of passengers based on their personal and travel details. This process is currently conducted manually. However, steps are currently being made to automate this process by, for example, using algorithms which systematically search for irregular patterns, or deviations from standard patterns.
- The third consideration relates to the understanding amongst airline companies as well as third parties who use these API data and must therefore adhere to the various requirements concerning the strict division between the currently API requirements, and the PNR Law currently under development. The PNR Law states that the airline companies must deliver Passenger Name Record (PNR) data. The PNR data include information that the airline companies need to make, process and check a reservation. Besides personal details such as the name and date of birth, the PNR data also include payment details, travel companions, baggage, and seating place in the airplane. The PNR Law was formally proposed in the national parliament on the 9th of January 2018. In the event that this law passes, airline companies will be obliged to collect data for each passenger and to pass these data on to two separate booths; once to the API Centre in the same manner as now, and three times to the Pi-NL booth. The Pi-NL booth requires PNR data as well as API data.

The fact that airline companies would need to provide API as well as PNR data (now only to the Customs and in future also based on the PNR-legislation) to the government does raise certain questions amongst airline companies regarding the efficiency and effectiveness of the new requirement. In other places in the world, the general practice is that there is one booth for passenger information; this is the case in the United States and the Gulf States, for instance. Airline companies in the Netherlands, as well as the sectoral organisation the IATA, lobby for a single window instead. If the PNR Law is passed and accepted, the Dutch authorities must collect passenger data using two channels, which forms an extra administrative burden for airline companies. The Dutch government is exploring the option of a single window to transfer the passenger information data.

Results of European developments

The API directive is part of a broader package of European measures to strengthen the borders of the internal market. API was the first element of this package. These measures arise in large part due to the pointed increase in the number of passengers entering Europe from third countries, and this trend is expected to be continued in the coming years (from 50 million non-EU passengers in 2015 to 76 million in 2025). The combination of having more passengers, as well as higher safety requirements have triggered the search for possibilities as to checking and processing large flows of passengers, without having to make concessions regarding safety requirements, or in respecting the rights of the passengers.

A few important recent developments and measures are brought together under the policy direction 'Smart Borders'. The measures involved include amongst others:

- Entry-Exit System (EES): In November of 2017, the Council of the European Union decided to introduce an EES, which would register all attempts by non-EU citizens, and non-registered EU citizens travelling into the Schengen area.
- European Travel Information and Authorization System (ETIAS): The Council of the European accepted a regulation on September 5th, 2018, stating that a European system for travel information and authorisation would be set up. The system is to be similar to the American Electronic System for Travel Authorization (ESTA). The system means that subjects of a third country who do not need a visa, must request travel authorization before they can travel into the Schengen zone.
- Systematic border control based on databases: On the 7th of March 2017, the Council for the European Union has accepted an amendment to the Schengen border code to sharpen the controls at the outer borders of the zone. The Member States will be obliged to systematically check all individuals at the borders of Schengen using relevant databases.
- Interoperability: Within the EU, work is being done to improve the interoperability of information systems such as EES, Visa Information System (VIS), ETIAS, and Schengen Information System (SISII). The rationale is that these systems will align with one another and allow for databases and systems to better use each other's information.
- Improving SISII: New categories for signalling and detecting are being added to the SISII.

When implementing EES and ETIAS it will be important in the context of carrier liability for airline companies to be able to assess whether someone has an ETIAS travel authorisation, and to be able to see whether the term of 90 days has not passed. Carrier liability entails being able to make the airline company accountable and responsible for ensuring that an individual is provided with a return flight in the event that they are not allowed into the Netherlands.

Comparable systems that check whether a passenger is permitted to cross the border of their country of destination before the departure of their flight are already in use in the United States, Canada, and Australia. These countries fall beyond the scope of the European API Directive, but can provide a possible approach that the EU could apply regarding the combined use of details and registers to assess the entrance of passengers. Airline companies receive an OK/NOT OK TO

BOARD signal before they board a plane. In doing so it is immediately clear whether a person will or will not be allowed to travel to the country of destination, and this reduces the risk to airline companies that they be made responsible for providing return flights for those passengers. Furthermore, this could contribute to the increase of safety on board because potentially dangerous individuals are not allowed on planes to begin with due to the existence of detection files and lists of risky individuals.

The expectation, and certainly the desire of the airlines, is that in the longer term, a single window for the delivery of passenger data will become a globally applied model. This is already the case in several countries. The API obligations are now included in the Netherlands in the Vreemdelingenwet 2000 and also apply to Dutch passengers. PNR-data are currently provided to the Customs and in the future also based on the PNR-legislation for the prevention and detection of serious crime and terrorism. Embedding the API and PNR obligations in one framework law on Civil Aviation Safety is, in our view, a logical route for the future. This would certainly increase the transparency for all parties involved.

1 Inleiding

1.1 Gebruik API-passagiersgegevens voor grenscontroles

Ten behoeve van grenscontroles en het tegengaan van illegale migratie zijn luchtvaartmaatschappijen verplicht om bepaalde gegevens van alle passagiers en bemanningsleden die van buiten het Schengengebied en van buiten de Europese Unie naar Nederland vliegen, te verstrekken aan de autoriteiten die belast zijn met grenscontrole. Het gaat om gegevens uit het reisdocument die worden aangevuld met enkele gegevens over de vlucht en de boeking. Deze verplichting heeft zijn basis in de Vreemdelingenwet (art. 4.3) en is verder uitgewerkt in het Vreemdelingenbesluit (art. 2.2a) en het Voorschrift Vreemdelingen (art. 2.1a). Met deze regelgeving heeft Nederland de EU Richtlijn 2004/82/EG geïmplementeerd.

Deze richtlijn staat bekend als de API-richtlijn. API staat voor Advance Passenger Information (API). 'Advance' verwijst naar het moment waarop de gegevens moeten worden verstrekt: namelijk aan het einde van de instapcontroles, dus voordat het vliegtuig naar Nederland vertrekt. Het stelt de autoriteiten, in casu de Koninklijke Marechaussee (KMar) in staat om tijdens de vlucht naar Nederland na te gaan of er mensen aan boord zijn die in het kader van de grenscontrole en tegengaan illegale migratie nadere aandacht behoeven. Het gaat bijvoorbeeld om mensen die illegaal het land willen binnenkomen, of om mensen die gesignaleerd staan in opsporingsregisters, watchlists of mensen die vanwege een combinatie van persoons- en vluchtgegevens matchen met een profiel.

Het doel van de verplichting is in artikel 1 van de API-richtlijn als volgt geformuleerd: (1) het verbeteren van de grenscontroles; en (2) de illegale immigratie bestrijden. In de toelichting op de richtlijn wordt gesteld dat 'verbetering van grenscontrole' zowel betrekking heeft op effectiviteit als efficiëntie[1]. Effectiviteit is hierbij te omschrijven als de mate waarin de inspanningen bijdragen aan het realiseren van de doelstellingen, efficiëntie duidt op de hoeveelheid middelen die worden ingezet om die doelstellingen te kunnen realiseren.

Het gebruik van API-gegevens heeft nog een aanvullend doel: de doorstroom van passagiers bij de grensdoorlaatposten bevorderen. Dit doel is in Nederland bij de implementatie toegevoegd (Nota van Toelichting, TK Jaargang 2012). Het controleren van een passagier, onder andere aan de hand van opsporingsregisters, kost namelijk tijd en kan opstoppingen aan de grensdoorlaatposten veroorzaken. Door vóór aankomst over gegevens te beschikken heeft de KMar meer tijd en mogelijkheden om op basis van opsporingsregisters, watchlisten en

[1] Nota van Toelichting. (Jaargang 2012). Besluit van 20 december 2012, houdende wijziging van het Vreemdelingenbesluit 2000 in verband met de uitbreiding van de vooraf door de luchtvervoerder te verstrekken passagiersgegevens (standaard API-set). Tweede Kamer de Staten Generaal 688.

profielen na te gaan of een passagier nadere aandacht behoeft[2]. Zij kan daardoor de grenswachten aan de doorlaatposten en/of de grenswachten die opereren in mobiele teams gericht laten uitkijken naar specifieke passagiers.

1.2 Nederlandse beleidscontext van het gebruik van API-gegevens

De noodzaak van een effectieve grenscontrole wordt al lang onderkend. In 2005 constateerde de Algemene Rekenkamer dat zowel wet- en regelgeving als de uitvoering van het grenstoezicht niet goed toegesneden waren op de bestrijding van terrorisme. De Rekenkamer concludeerde dat een risicogestuurde aanpak van personencontroles en de organisatie van de informatie-uitwisseling tussen de verschillende diensten verder ontwikkeld moesten worden (Algemene Rekenkamer, 2005). In 2006 presenteerden de ministers van Vreemdelingenzaken en Integratie, Justitie, Binnenlandse Zaken, Defensie en de staatssecretaris van Financiën, daarop een pakket aan maatregelen, met onder andere als doel beter zicht te krijgen op passagiers- en goederenstromen en handhaving en toezicht gerichter (risicogestuurd) uit te voeren. Eén van de maatregelen betrof een onderzoek naar mogelijkheden, nut en noodzaak van inname van door vervoerders verstrekte pre-arrival persoonsgegevens (Minister van Vreemdelingenzaken en Integratie e.a., 2006).

Een jaar later kwam de 'Werkgroep organisatie passagiersgegevens Schiphol' (Commissie Gerritse), met een rapport. Zij stelde vooral ook het belang van een goede doorstroom aan de controleposten aan de orde. De werkgroep onder leiding van de Secretaris Generaal van het Ministerie van Financiën, constateerde dat de groeiende passagiersaantallen vaker leiden tot opstoppingen bij de verschillende controlepunten op de luchthaven. Onder de noemer 'Project Redesign Passenger Proces' werden aanbevelingen gedaan om dit zoveel mogelijk te beperken. Zij deed aanbevelingen van organisatorische aard gericht op de verbetering van de afstemming tussen KMar, Douane, Luchthaven Schiphol, en luchtvaartmaatschappijen. Ook beval de commissie aan om verder te gaan met de ontwikkeling van geautomatiseerd toezicht en informatiegestuurd en risicogericht optreden op basis van vooraf ontvangen passagiers gerelateerde informatie (Gerritse, 2007).

In 2008 is het Programma Vernieuwing Grensmanagement (PVG) gestart. In het kader van dit programma werden vier projecten uitgevoerd:

- Passenger Related Data Exchange (PARDEX): dit project had tot doel gezamenlijk voorstellen te ontwikkelen om de bij het programma betrokken organisaties in staat te stellen om in onderlinge samenwerking sneller, slimmer en beter passagiersgerelateerde informatie te verzamelen, te analyseren en

[2] Dit is per 7 april 2017 expliciet opgenomen in de Schengen Grenscode, artikel 8 lid 2, waarin staat: De controles aan de hand van de databanken (…) kunnen vooraf worden uitgevoerd op basis van passagiersgegevens die worden ontvangen overeenkomstig Richtlijn 2004/82/EG.

te verspreiden, teneinde de veiligheid en mobiliteit in en rond het passagiersverkeer te vergroten.
- Advance Passenger Information (Project API): implementatie van de EU richtlijn 2004/82/EG.
- Automatische Grenspassage (Project No-Q): het project No-Q had als doel het realiseren van een snel en integer concept voor automatische grenspassage. Het primaire doel was om in 2010 aan EU-onderdanen (inclusief Zwitserland) die het Schengengebied via Schiphol verlaten de mogelijkheid te bieden om zelf, geholpen door innovatieve ICT-oplossingen, de grenspassage te verzorgen zonder actieve tussenkomst van een ambtenaar belast met grensbewaking.
- Registered Travellers Programs: ontwikkeling van een systeem dat de mogelijkheid biedt om geautomatiseerd de grens te kunnen passeren. Het programma is bedoeld voor bepaalde passagiers waarover vooraf persoonsgegevens, biometrische kenmerken en antecedenten zijn verzameld.

In 2009 bood de minister van Veiligheid en Justitie het Kaderdocument grenstoezicht aan. In dit document wordt geconstateerd dat op verschillende plekken werd gewerkt aan de verbetering van de grenscontrole. In het Kaderdocument wordt de ambitie uitgewerkt om hier een planmatige samenhang in aan te brengen. In het document wordt ook een 'concentrische bandering' voorgesteld: effectief grenstoezicht begint in de landen van herkomst. Grenstoezicht in Nederland moet ondersteund worden met bij vertrek uit het land van herkomst verkregen informatie. Deze informatie moet de autoriteiten in staat stellen te komen tot integrale risicoprofielen op basis waarvan gerichter controles kunnen worden uitgevoerd. Het document stelt dat stelselmatige maar ook steekproefsgewijze controles alleen, niet meer van deze tijd zijn.

> *'We moeten er meer en meer naar toe dat de grensautoriteiten zich bij de controles meer kunnen richten op de met een als hoog risico bestempelde passagiers en hun bagage, terwijl de passagiers met een laag risico met minimaal oponthoud de grens vlot kunnen passeren'* aldus het kaderdocument (Ministerie van Justitie, 2009).

De ontwikkeling van de API-verplichting binnen Nederland en de EU zijn altijd aangesloten geweest op de ontwikkeling van een API richtlijn in breder internationaal verband, waar ook landen buiten de EU aan gebonden zijn. Deze richtlijn is in de jaren tachtig opgesteld en verder ontwikkeld door de International Civil Aviation Organization (ICAO)[3], World Customs Organization (WCO) en International Air Transport Association (IATA). ICAO en IATA[4] doen dat tegen de achtergrond van hun bredere doelstelling om het vliegverkeer veiliger te maken en vooral ook om voorschriften internationaal te standaardiseren, zodat zij voor luchtvaartmaatschappijen beter zijn na te leven.

[3] ICAO Annex 9, Chapter 9 en UN Security Council, resolutie 2178, paragraaf 9
[4] IATA is een belangenorganisatie van de luchtvaartmaatschappijen en is bij de ontwikkeling van de richtlijn als waarnemer betrokken

1.3 Van pilot tot verplichting

Medio 2008 is onder verantwoordelijkheid van het ministerie van Veiligheid en Justitie gestart met de tweede van bovengenoemde vier PVG projecten: de bouw van een testprogramma voor API. Doelstellingen van deze 'API-pilot' waren:

1. De toepassing van de API-richtlijn door API-gegevens op te vragen van één of meer luchtvaartmaatschappijen,
2. Het beproeven op welke wijze de verschillende overheidspartijen API-gegevens het beste kunnen ontvangen en wat daarvoor nodig is en
3. Het beproeven van de effectiviteit en meerwaarde van het gebruik van API-gegevens voor de realisatie van een effectiever grenstoezicht (Ministerie van Veiligheid en Justitie, Evaluatierapport inzake het gebruik van API, 2013).

Op 16 december 2009 is gestart met een pilot naar de verwerking en het gebruik van API-gegevens met een kleiner aantal datavelden dan nu. Aanvankelijk nam alleen de KLM daaraan deel. De luchtvaart-maatschappij startte met het verzamelen van gegevens van inkomende vluchten die vertrokken waren van twee Turkse luchthavens en breidde dit aantal in de loop van de pilot uit tot 83 inkomende vluchten afkomstig van veertien luchthavens (Ministerie van Veiligheid en Justitie, 2013). Alle luchtvaartmaatschappijen werden per 1 januari 2012 verplicht API-gegevens te verstrekken voor vluchten van buiten Schengen naar de EU. In eerste instantie beperkte die verplichting zich tot vluchten vanaf 28 luchthavens die uit het oogpunt van illegale immigratie als risicovol werden aangemerkt. Sinds juni 2016 is dit uitgebreid en geldt de API-verplichting voor alle vluchten en alle passagiers die van buiten Schengen aankomen op een Nederlandse luchthaven. In tabel 1 is de ontwikkeling van de API-verplichting op hoofdlijnen geschetst.

In de ontwikkeling van het Nederlandse API-systeem worden drie fases onderscheiden: API-1, API-2 en het huidige API-3. API-1 verwijst naar het systeem uit de pilotfase. Het betrof een relatief eenvoudig systeem dat nog geen directe koppeling met databanken had. API-2 verwijst naar de fase waarin het aanleveren van de gegevens verplicht werd gesteld en de gegevensset werd uitgebreid alsmede het aantal vluchten. Op 31 maart 2017 is de ontwikkeling afgerond. Sindsdien spreekt men van API-3. Er is nu een directe koppeling met databestanden zoals het Schengeninformatiesysteem II (SISII), het Opsporingssysteem (OPS) en watchlists. Op dit moment wordt nog gewerkt aan de (automatische) koppeling met het register van vermiste reisdocumenten Stolen and Lost Travel Documents Database (SLTD) van INTERPOL.

In 2014 is het gebruik van API-gegevens ten behoeve van de Nederlandse grenscontrole voor het eerst geëvalueerd. Het rapport beschrijft de ontwikkeling van het API-systeem en beschrijft ook de achtergronden. Ook worden de perspectieven geschetst die het gebruik van API-gegevens op termijn bieden.

In de evaluatie die destijds naar de Tweede Kamer is gestuurd is de volgende conclusie geformuleerd:

> *'Conclusies over de effectiviteit voor de grensbewaking en het tegengaan van illegale immigratie zijn zeker wel te trekken op basis van de ervaringen tot nu toe, maar de effecten van het gebruik van API zijn niet in cijfers te kwantificeren. Kwantificeren zal ook in de toekomst niet goed mogelijk zijn, omdat op het resultaat van de grenscontroles ook zeer veel andere factoren van invloed zijn.'*

Wel constateert men een hoog niveau van naleving bij luchtvaartmaatschappijen. Verder bleek dat de KMar in het gebruik van API-gegevens een belangrijk ondersteunend middel heeft gevonden voor de effectievere inzet van het personeel aan de grens; het bleek vooral nuttig voor een meer gerichte inzet van gatecontroles. De evaluatie wees er tegelijk ook op dat door verschillende technische beperkingen van het toen operationele API-systeem (API-1) geen mobiliteitswinst (snellere controles) bij de grensbalies kon worden geboekt.

Op basis van de bevindingen besloot de staatssecretaris tot een aantal aanpassingen in beleid- en regelgeving die ook zijn doorgevoerd. De aanpassingen betreffen (Brief van de staatssecretaris, 25 juli 2014):

- De bewaartermijn van API-gegevens wordt voor bepaalde gevallen verlengd met drie dagen. De verlenging heeft betrekking op gegevens van derdelanders met een risico op illegale immigratie.
- Er wordt een plan opgesteld voor uitbreiding van het aantal inkomende vluchten waarvoor luchtvaartmaatschappijen gegevens moeten verstrekken. De uitbreiding wordt gebaseerd op plaatsen van herkomst met een verhoogd risico op illegale immigratie.
- De transparantie wordt vergroot over het gebruik van API-gegevens. In de Vreemdelingencirculaire wordt expliciet vermeld dat bij grenscontroles die ondersteund worden door API, gebruik wordt gemaakt van risicoprofielen.

Voorliggend onderzoek komt voort uit de resultaten van de evaluatie en de toegezegde aanpassingen. Sinds de laatste evaluatie zijn er nog andere vragen naar voren gekomen die het ministerie van Justitie en Veiligheid beantwoord wilde hebben. Deze vragen zijn opgenomen in de volgende paragraaf. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is de opdrachtgever van dit onderzoek.

tabel 1 Ontwikkeling API-richtlijn en de Nederlandse verplichting voor luchtvaartmaatschappijen om verplicht API-gegevens te verstrekken

1 juli 1988	ICAO, WCO en IATA adviseren het gebruik van API-gegevens aan t.b.v. grenscontrole.
29 april 2004	In EU-verband wordt de API-richtlijn aangenomen.
9 juli 2007	Wet opname API-richtlijn in de Nederlandse Vreemdelingenwet. Wettelijke vereiste om luchtvaartmaatschappijen te verplichten API-gegevens te verstrekken.
2008	Start Programma Vernieuwing Grensmanagement
16 december 2009	Start pilot met ontvangst en verwerking van een berperkte set van 9 API-gegevens van vluchten van de KLM.
1 januari 2012	Het verstrekken van API-gegevens wordt verplicht gesteld op vluchten vanaf 28 luchthavens[5]
29 december 2012	API-set wordt uitgebreid met 5 gegevens
1 april 2013	API-verplichting uitbreiding naar 54 luchthavens[6]
28 september 2015	API-verplichting uitbreiding naar 132 luchthavens[7]
1 juli 2016	API-verplichting wordt uitgebreid naar alle vluchten en alle passagiers naar Nederland van buiten het EU- en Schengengebied.[8]

1.4 Doel van dit onderzoek

Met voorliggend onderzoek is nagegaan hoe de verplichtingen met betrekking tot het gebruik van passagiersgegevens in de praktijk worden nageleefd door alle schakels die een rol spelen. Het onderzoek concentreert zich op de verplichtingen die de *Nederlandse* autoriteiten aan vervoerders opleggen. Omdat veruit de meeste vluchten van buiten het Schengengebied en van buiten de EU naar Nederland, Schiphol als bestemming hebben, concentreert dit onderzoek zich op de praktijk bij de KMar op Luchthaven Schiphol. Hiervoor is gekozen omdat ruim 95% van de passagiersstromen van buiten Schengen (waarbij API een rol speelt) via deze luchthaven verloopt. In tabel 2 is een voorbeeld gegeven van de zomerdienstregeling in 2018 met het aantal vluchten en de fractie API-plichtige vluchten. Het gaat in deze tabel om de inkomende vluchten. De andere luchthavens zijn wel opgenomen waar het gaat om de analyse van het aantal passagiers en de aan API gerelateerde signaleringen.

[5] Staatscourant 27-10-2011
[6] Staatscourant 8-11-2012
[7] Staatscourant 28-9-2015
[8] Staatscourant 24-6-2016

tabel 2 Voorbeeld zomerregeling 2018 dag 1, inkomende vluchten

Luchthaven	Aantal vluchten	API-plichtige vluchten	Percentage API-plichtige vluchten
Schiphol	730	141	19%
Eindhoven	56	4	7%
Rotterdam	25	1	4%
Maastricht	3	1	33%
Groningen	10	1	10%
Alle luchthavens	824	148	18%

Bron: KMar

Met dit onderzoek is zowel gekeken naar het *proces* van gegevensverwerking als naar het *effect* en de *meerwaarde* ervan. In het kader van de evaluatie van het *proces* is nagegaan hoe passagiersgegevens door luchtvaartmaatschappijen worden verzameld en doorgegeven, en vervolgens door de KMar worden gebruikt. In het kader van de evaluatie van het *effect* en de *meerwaarde* is gekeken naar cijfers die betrekking hebben op het gebruik van de passagiersgegevens, onder meer naar de frequentie waarmee die gegevens leiden tot interventies aan de grens. In het onderzoek zijn het proces en de meerwaarde verder geïllustreerd aan de hand van geanonimiseerde casuïstiek.

In dit onderzoek zijn ook toekomstige ontwikkelingen betrokken. Onder meer wordt in beeld gebracht hoe de verplichting voor vervoerders om passagiersgegevens te verstrekken zich verhoudt tot mogelijk toekomstige verplichting voor dezelfde vervoerders om Passenger Name Record (PNR-gegevens) te verstrekken[9]. Deze verplichting is neergelegd in een wetsvoorstel (PNR-wet) dat afgelopen januari aan de Tweede Kamer is aangeboden. De PNR-wet is gericht op het opsporen en bestrijden van ernstige criminaliteit en terrorisme.

Daarnaast wordt gekeken naar andere ontwikkelingen die verband houden met grenscontroles, zoals de invoering van een Entry-Exit System (EES) waarmee in- en uitreis van passagiers van buiten de EU kan worden gevolgd, en het European Travel Information and Authorisation System (ETIAS). ETIAS is een Europees reisinformatie en –autorisatiesysteem gericht op niet-visum-plichtige derde-landers. Op dit moment geldt dat voor 61 landen[10]. ETIAS is goed te vergelijken met het ESTA systeem zoals de Verenigde Staten toepassen.

De twee centrale onderzoeksvragen die met dit onderzoek worden beantwoord zijn:

- Wat kan gezegd worden over het gebruik en de effectiviteit van API-gegevens ten behoeve van het grenscontrole en het tegengaan van illegale immigratie en op welke wijze is gevolg gegeven aan eerdere aanbevelingen ten aanzien van API?

[9] PNR-gegevens bevatten informatie die luchtvaartmaatschappijen nodig hebben om reserveringen te kunnen verwerken en te controleren. Naast persoonsgegevens als naam, geboortedatum, gaat het om bijvoorbeeld betalingsgegevens, reisgenoten, bagage, en plaats in het vliegtuig.
[10] https://www.schengenvisainfo.com/etias/

- In hoeverre kunnen recente relevante Europese ontwikkelingen gevolgen hebben voor de wijze waarop API-gegevens in Nederland gebruikt worden?

Deze twee hoofdvragen zijn uitgewerkt in veertien deelvragen. Deze zijn op hun beurt uitgewerkt tot vraagpunten voor de interviews.

1. In hoeverre leven luchtvaartmaatschappijen de API-gerelateerde verplichtingen sinds 2013 na?
2. Hoe verloopt de samenwerking tussen de KMar, luchtvaartmaatschappijen en eventuele andere partijen bij het ontvangen van API-gegevens?
3. In hoeverre en op welke wijze worden API-gegevens sinds 2013 gebruikt: A) bij grens- en gatecontroles (zowel balie als e-gates)? B) Bij het 'claimen' van een passagier aan wie de toegang is geweigerd (artikel 65 Vw2000)? C) in het kader van identiteitsvaststelling van ongedocumenteerden (waaronder asielzoekers) of om de nationaliteit en de herkomst van een persoon te bepalen?
4. Hoe heeft het aantal API-gerelateerde vluchten, -passagiers, -hits, interventieberichten, interventies en toegangsweigeringen zich sinds 2013 ontwikkeld?
5. Een bredere set API-gegevens worden ook in het Travel Information Portal (TRIP) verwerkt. Hoe verhoudt het API-gebruik in TRIP zich tot het API-gebruik in het API-Centrum van de KMar?
6. Wat zijn de ervaringen van betrokken partijen ten aanzien van het API-gebruik en het API-3 systeem? Wat gaat goed en wat kan beter en op welke manier?
7. Zijn de aanpassingen conform toezegging in de brief aan de Tweede Kamer en de afspraken in de bestuursovereenkomst tussen het ministerie van Veiligheid en Justitie en het ministerie van Defensie uitgevoerd? Indien dit niet het geval is, waarom niet?
8. In hoeverre is het gebruik van API-gegevens sinds 2013 van invloed op: a) het verbeteren van de grenscontroles? (o.a. kwaliteit, efficiëntie, mobiliteit, bedrijfsvoering) b) het bestrijden van illegale immigratie? (o.a. toegangsweigeringen, bestrijding van mensenhandel/-smokkel).
9. In hoeverre en op welke wijze zijn andere factoren (dan het API-gebruik) van invloed op het verbeteren van de grenscontroles en/of het bestrijden van illegale immigratie?
10. Indien het API-gebruik geen invloed heeft op het verbeteren van de grenscontroles en/of het bestrijden van illegale immigratie, wat zijn daarvan dan de redenen? In hoeverre en op welke wijze kan dit worden verbeterd?
11. Is er sprake van onverwachte effecten van het API-gebruik? Zo ja, welke?
12. API-gegevens worden momenteel vergeleken met SISII en het OPS ten behoeve van het verbeteren van het grensbeheer. In hoeverre leidt de vergelijking van API-gegevens met SISII en OPS maar ook met zogeheten watchlists tot een betere grenscontrole?
13. Hebben recente Europese ontwikkelingen gevolgen voor de wijze waarop API-gegevens in Nederland gebruikt kunnen worden?

Belangrijke ontwikkelingen zijn het (toekomstige) gebruik van andere gegevens, zoals EES[11], ETIAS[12], PNR[13], interoperabiliteit[14] en veranderingen in Schengenregelgeving zoals de introductie van systematische checks van EU-burgers in de databases[15].

14. Gelet op bovenstaande ontwikkelingen: a) In hoeverre kan API-gebruik toegevoegde waarde hebben wat betreft de openbare orde en veiligheid? b) In hoeverre kan API-gebruik toegevoegde waarde hebben indien dit ook betrekking heeft op uitreizen? c) In hoeverre kan interactieve API toegevoegde waarde hebben?

1.5 Aanpak

De belangrijkste informatiebron voor dit onderzoek bestaat uit de mensen die dagelijks werken met passagiersgegevens. Wij spraken medewerkers van drie Nederlandse luchtvaartmaatschappijen en de KMar.

Bij *luchtvaartmaatschappijen* spraken wij met compliance- en veiligheidsfunctionarissen en mensen die de grondafhandeling aansturen of verantwoordelijk zijn voor de uitbesteding daarvan. De gesprekken zijn gevoerd aan de hand van een half gestructureerde vragenlijst. Doel van de gesprekken was een beeld krijgen van het werkproces waarmee API-gegevens worden verzameld en doorgegeven aan de KMar. Specifieke aandachtpunten in de gesprekken waren: het proces dat loopt van (online) ticketverkoop tot het vertrek van het toestel, naleving (frequente en omstandigheden waaronder de verplichting niet wordt nageleefd), de wijze waarop betrouwbaarheid van gegevens wordt geborgd en de samenwerking met de KMar. In de gesprekken is door de respondenten vaak ook ingegaan op hoe in andere landen de uitvoering van de API-richtlijn is vormgegeven.

Bij de KMar hebben wij gesproken met mensen van het Targeting Center Borders (TCB) en het daaronder vallende API-Centrum die passagiersgegevens vergelijken; met medewerkers bij de Sectie Analyse & Onderzoek (A&O) van de Afdeling Intelligence die de geanonimiseerde data analyseren; en met mensen van Brigade Grensbewaking en Dedicated Gate Control (DGC) die op basis van signaleringen al dan niet tot actie overgaan.

Bij het TCB is gesproken over hoe men op basis van een match met een opsporingsdatabase, watchlist of profiel uiteindelijk komt tot een alert. Ook is gesproken over hoe alerteren gaat op basis van profielen en welke afspraken zijn gemaakt met de Brigade Grensbewaking en DGC over opvolging van alerts. Met Brigade Grensbewaking is vervolgens gesproken over het laatste stuk van het API-proces, namelijk de

[11] Verordening 2017/2226 voor oprichting van een In en Uitreissysteem, 30 november 2017
[12] Voorstel COM (2016) 731 voor een Verordening tot instelling van een Europees Systeem voor reisinformatie en –autorisatie (ETIAS)
[13] Richtlijn 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit
[14] Voorstellen (2017) 793 en 794 betreffende de vaststelling van een kader voor interoperabiliteit tussen EU-informatiesystemen
[15] Verordening 2017/458 van 15 maart 2017 tot wijziging van Verordening 2016/399 inzake het aanscherpen van de controles aan de hand van relevante databanken aan de buitengrenzen.

doorgifte van alerts aan de grenswachten die de doorlaatposten bemensen.

De onderzoekers hebben bij DGC twee ochtenden meegelopen op de luchthaven Schiphol. De gesprekken die de onderzoekers voerden waren casusgericht. Dat wil zeggen dat niet zozeer werd gevraagd naar algemene ervaringen maar dat aan de hand van concrete casussen/dossiers is nagegaan op wat voor soort passagiers alerts betrekking hebben en hoe daarop wordt gereageerd. Met de medewerkers zijn de alerts doorgenomen die zij dagelijks doorgemaild krijgen van het API-Centrum. Daarmee is een beeld gevormd van hoe de alerts worden beoordeeld en welke afwegingen worden gemaakt om wel of niet in actie te komen. De twee meeloopochtenden leverden een beeld op achter de cijfers.

Een andere bron zijn de beleidsmakers van het ministerie van Justitie en Veiligheid (waaronder de Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV) en die van het ministerie van Infrastructuur en Waterstaat, vanwege hun kennis over de achtergronden van wettelijke voorschriften en hun kennis over het internationale krachtenveld waarin internationale afspraken tot stand komen. Onderstaande tabel geeft een overzicht van de geïnterviewde organisaties. De bijlage bevat een detailoverzicht van respondenten.

tabel 3 overzicht van organisaties waarmee is gesproken

	Onderdelen
Luchtvaartmaatschappijen	Drie Nederlandse luchtvaartmaatschappijen: - Corendon - KLM - Transavia
Brancheverteegenwoordiging	- IATA
Koninklijke Marechaussee	- Staf CKMar - Targeting Center Borders (API-Centrum) - Afdeling Intelligence (Sectie Analyse & Onderzoek) - Dedicated Gate Control - Brigade Vreemdelingenzaken - Brigade Grensbewaking Schiphol
Rijksoverheid (ministeries)	- Ministerie van Justitie en Veiligheid, Directie Migratiebeleid - Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) - Ministerie van Infrastructuur en Waterstaat

Naast de gesprekken bij de KMar (Targeting Center Borders) is informatie verzameld over het gebruik van passagiersgegevens. Aan de hand van deze kwantitatieve informatie zijn ontwikkelingen beschreven van het aantal vluchten/reizigers/matches/hits/alerts dat uit de verwerking van passagiersgegevens is voortgekomen. Er is ook beschreven waarmee die informatie verband houdt.

Voor dit onderzoek is verder gebruik gemaakt van schriftelijke bronnen. In de eerste plaats zijn dat de Nederlandse wetsteksten zoals opgenomen in onder andere de Vreemdelingenwet, de EU Directive API en de richtlijn van ICAO[16] en de verschillende toelichtingen die daarop zijn gegeven. Een belangrijk document in dit kader is de Nota van Toelichting bij het besluit van 20 december 2012 waarin de staatsecretaris van Veiligheid en Justitie het doel van het gebruik van API-gegevens toelicht[17].

Aanvullend zijn documenten in de studie betrokken die de verantwoordelijke ministeries (met name het ministerie van Justitie en Veiligheid) hebben opgesteld over grenscontroles en grensbeheer. Twee belangrijke documenten zijn het Kaderdocument waar in paragraaf 1.2 naar is verwezen en de eerder uitgevoerde evaluatie van het gebruik van API-gegevens.

Tenslotte zijn ook studies van derde partijen betrokken, zoals een onderzoek dat op Europees niveau is uitgevoerd naar hoe de lidstaten de richtlijn hebben geïmplementeerd, de studie van de Algemene Rekenkamer, de position papers van IATA en enkele academische publicaties, waaronder een proefschrift over de rol van private vervoerders bij grenscontroles (Scholten, 2014). Ten aanzien van de literatuurstudie moet worden opgemerkt dat de beschikbaarheid van publicaties beperkt is en dat publicaties snel gedateerd zijn vanwege de snelheid waarmee het gebruik van API-gegevens zich ontwikkelt.

Dit onderzoek kent enkele beperkingen. Er zijn in overleg met de begeleidingscommissie drie luchtvaartmaatschappijen geselecteerd. Dit zijn alleen Nederlandse maatschappijen. De ervaringen van buitenlandse maatschappijen met de Nederlandse implementatie van API hebben we daardoor beperkt in kaart kunnen brengen. Op basis van de beschikbare registraties over de periode vanaf 2013 tot en met maart 2018 is het niet mogelijk een volledige kwantitatieve effectevaluatie te maken. In deze periode zijn veel veranderingen te noteren. Het aantal vluchten, het aantal gegevens is gestegen en de kwaliteit van de verschillende registers verbeterd en de systemen die in gebruik zijn bij TCB zijn eveneens verbeterd. Voor deze evaluatie hebben we tellingen ontvangen over het aantal vluchten, reizigers, matches-hits-alerts, de bronnen van de match en de terugkoppeling op de alerts. Deze gegevens hebben we per maand en per luchthaven via de KMar ontvangen. De tijdreeks die beschikbaar is omvat niet op alle onderdelen data en gedurende deze periode is een aantal systematische wijzigingen opgetreden. De jaren zijn daardoor niet zuiver te vergelijken. Bovendien kunnen we niet per individuele match-hit-alert het hele proces volgen tot en met terugkoppeling.

[16] WCO/IATA/ICAO Guidelines on Advance Passenger Information, 2014
[17] Nota van Toelichting. (Jaargang 2012). Besluit van 20 december 2012, houdende wijziging van het Vreemdelingenbesluit 2000 in verband met de uitbreiding van de vooraf door de luchtvervoerder te verstrekken passagiersgegevens (standaard API-set). Tweede Kamer de Staten Generaal 688.

De efficiëntie is in deze evaluatie kwalitatief beschreven. Cijfers over aantallen mensen en middelen die direct aan API zijn toe te schrijven en de eventuele besparing ten opzichte van een situatie zonder API zijn niet verzameld en geanalyseerd voor deze evaluatie. We hebben ons daarom beperkt tot de ervaringen die met name KMar heeft en de luchtvaartmaatschappijen.

1.6 Opbouw van dit rapport

In hoofdstuk 2 wordt beschreven wat de verplichtingen in het kader van de API-richtlijn inhouden en wat de achterliggende doelen daarvan zijn. Hierbij wordt ook expliciet stilgestaan bij de voorwaarden waaronder de gegevens mogen worden gebruikt, de zogenoemde doelbinding en de beoogde functionaliteit van API. We beantwoorden hier de vraag *hoe* API-gegevens verondersteld worden bij te dragen aan betere grenscontrole. In dit hoofdstuk wordt vervolgens ook ingegaan op hoe de verplichting om API-gegevens te verstrekken zich verhoudt tot de toekomstige verplichting om PNR-gegevens te verstrekken. En hoe de API-verplichting zich verhoudt tot de Carrier Liability: een Europese Richtlijn[18] die vervoerders o.a. verplicht te controleren of passagiers over de juiste reisdocumenten beschikken. Ook de Schengengrenscode krijgt aandacht, omdat daarin is beschreven wat de grenscontrole verplichting inhoudt en hoe API gegevens daaraan moeten bijdragen.

Hoofdstuk 3 gaat in op hoe het verzamelen en verstrekken van passagiersgegevens in de praktijk gebeurt. Het proces wordt beschreven dat luchtvaartmaatschappijen hebben ingericht, dat loopt van het moment dat iemand een vlucht boekt tot aan het moment dat het vliegtuig opstijgt met bestemming Nederland. Vervolgens wordt beschreven hoe de gegevens door de KMar worden verwerkt en ook hoe aan de hand van signalen wordt geacteerd. Er wordt hierbij onderscheid gemaakt tussen de manier waarop het API-Centrum data vergelijkt en de manier waarop vervolgens door grenswachters daarop wordt geacteerd. De beschrijving van het proces wordt aangevuld met cijfermatige overzichten die in meer detail in de bijlage zijn opgenomen.

Hoofdstuk 4 bevat de evaluatie van het gebruik van API-gegevens en het vernieuwde API systeem. In de eerste plaats wordt de meerwaarde geëvalueerd. Als referentiepunt gebruiken we hier de veronderstellingen die aan de API-richtlijn en de Nederlandse verplichting ten grondslag liggen, namelijk dat API-gegevens helpen bij het verbeteren van de grenscontrole en tegengaan van illegale migratie. Vervolgens wordt in dit hoofdstuk beschreven hoe de meerwaarde kan worden vergroot. We baseren ons hierbij met name op wat de partijen die betrokken zijn bij API, daarover in de interviews naar voren hebben gebracht.

Het rapport besluit met een conclusie waarin de onderzoeksvragen waar mogelijk worden beantwoord.

[18] Richtlijn 2001/51/EG

2 API-richtlijn en actuele ontwikkelingen

2.1 Inleiding

In Nederland is de API-richtlijn geïmplementeerd in de Vreemdelingenwet. In dit hoofdstuk wordt beschreven wat dat betekent. We gaan in op wat wordt verstaan onder grenscontrole en illegale immigratie. Ook wordt beschreven welke verplichtingen samenhangen met de API-richtlijn. Luchtvaartmaatschappijen hebben namelijk ook nog andere verplichtingen om de effectiviteit van de grenscontrole te ondersteunen. Bijvoorbeeld de verplichting om te controleren of passagiers over de juiste reisdocumenten beschikken (carrier liability). Hoewel deze verplichting losstaat van de verplichting om API-gegevens te verstrekken, draagt zij er in de praktijk wel aan bij dat API-gegevens een hoge betrouwbaarheid hebben.

In dit hoofdstuk bespreken we ook de Europese PNR-richtlijn en de Schengengrenscode. De Europese PNR-richtlijn zou in Nederland met de PNR-wet worden geïmplementeerd. De behandeling van het wetsvoorstel van januari 2018 is in de Tweede Kamer tot nader order uitgesteld[19]. Met deze wet zouden luchtvaartmaatschappijen ook verplicht worden om gegevens te verstrekken aan Nederlandse autoriteiten ten behoeve van het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

2.2 Doelbinding API

API-gegevens worden gebruikt ter verbetering van de grenscontroles en het tegengaan van illegale immigratie. De API-richtlijn definieert in artikel 2 grenscontrole als volgt:

> *'De controle aan de grenzen welke, onafhankelijk van enige andere aanleiding, uitsluitend op grond van de beoogde grensoverschrijding wordt uitgeoefend.'*

De Schengengrenscode[20], die directe werking heeft voor lidstaten en de grensautoriteiten, stelt regels voor de uitoefening van grenscontroles. Bepaald is onder andere dat landen aan hun Schengenbuitengrens de controle *systematisch* uitvoeren. Dit houdt in dat iedere grenspassant moet worden gecontroleerd.

[19] Wetsvoorstel implementatie EU richtlijn persoonsgegevens van luchtvaartpassagiers, 9 januari 2018
[20] Verordening 2016/399 betreffende een Uniecode voor overschrijding van de grenzen door personen.

Voor passagiers die van buiten het Schengengebied op een Nederlandse luchthaven aankomen, betekent dit dat zij onder andere door de KMar gecontroleerd moeten worden op de volgende punten (art. 8 Schengengrenscode):

- identiteit op basis van de overgelegde of getoonde reisdocumenten;
- echtheid en geldigheid van het reisdocument;
- of het reisdocument geregistreerd staat in de Stolen and Lost Traveldocuments Database (SLTD);
- of de passagier voorkomt in het Schengen Informatie Systeem II (SISII) en/of Opsporingssysteem (OPS);
- of hij/zij voldoet aan de voorwaarden voor binnenkomst, o.a. voldoende middelen van bestaan heeft (voor onderdanen van een derde land);
- plaats van vertrek en de plaats van bestemming van de betrokken onderdaan van een derde land, alsmede het doel van het voorgenomen verblijf;
- aanwezigheid van visum of verblijfsvergunning (voor onderdanen van een derde land).

Op de Nederlandse luchthavens vindt bij vertrekkende passagiers systematische controle plaats bij de grensdoorlaatposten. Deze controle houdt onder andere in dat reisdocumenten worden gescand en de gegevens worden vergeleken met SISII, OPS en SLTD. Bij aankomende passagiers van buiten Schengen wordt deze systematische grenscontrole ten behoeve van doorlooptijd en kwaliteit, ondersteund door het API-Centrum. Hoe dat precies gebeurt wordt beschreven in paragraaf 2.3.

2.3 Uitgangspunt van API

Nederland heeft de API-richtlijn als verplichting overgenomen in de Vreemdelingenwet 2000 en verder uitgewerkt in het Vreemdelingenbesluit en het Voorschrift Vreemdelingen. Opmerkelijk is dat daarmee in de Vreemdelingenwet bepalingen zijn opgenomen die ook van toepassing zijn op Nederlanders. In tabel 2 is een overzicht gegeven wat er concreet wordt voorgeschreven met de wet, het onderliggende besluit en voorschrift.

tabel 4 Wettelijk kader API

	Artikel	*Strekking van het artikel*
Vreemdelingenwet	Art. 4.3	Vervoerders kunnen verplicht worden gesteld om gegevens van passagiers die zij vervoeren te verstrekken aan de ambtenaren die belast zijn met de grensbewaking.
Vreemdelingenbesluit	Art. 2.2a	Het gaat om de volgende gegevens (art 2.2a lid 3): • nummer van het reisdocument • aard van het reisdocument • nationaliteit • volledige naam • geboortedatum • geslacht • staat van afgifte van het reisdocument • vervaldatum • vluchtnummer • tijdstip van vertrek en aankomst van het vervoersmiddel • aantal met dat vervoermiddel vervoerde passagiers • grensdoorlaatpost van binnenkomst • eerste instappunt • overige reisroutegegevens • Passenger Name Record-bestandslocatie In art. 2.2a van het Voorschrift Vreemdelingen is voorgeschreven dat het gaat om gegevens van alle passagiers die vanaf een luchthaven die niet in de Europese Unie of een land dat betrokken is bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis gelegen is, naar Nederland reizen. Vervoerder vernietigt de gegevens binnen 24 uur na aankomst in Nederland. Autoriteit belast met grensbewaking doet dit binnen 24 uur na binnenkomst van de passagier.
Voorschrift Vreemdelingen	Art. 2.1a	De vervoerder zendt de verzamelde passagiersgegevens elektronisch, voor het einde van de instapcontroles aan de ambtenaar belast met de grensbewaking. In het derde lid van het artikel is aangegeven dat de gegevens moeten worden verstrekt volgens een bepaalde indeling (EDIFACT/PAXLST).

In de nota van toelichting bij het besluit waarmee het verstrekken van API-gegevens verplicht wordt gesteld, is aangegeven dat het doel tweeledig is. Zowel de grenscontrole verbeteren als opstoppingen aan de grensdoorlaatposten beperken (Nota van Toelichting, TK Jaargang 2012).

Hoe API geacht wordt de grenscontrole te verbeteren

API moet bijdragen aan de effectiviteit van de grenscontrole. Door de controle voor een deel al uit te voeren door het API-Centrum op het moment dat de passagier nog onderweg is, is er meer tijd om onderzoek te doen naar een passagier. Er kan bijvoorbeeld worden nagegaan of en met wie de persoon samen reist en er kunnen eventueel aanvullende openbare bronnen worden geraadpleegd. Ook is er meer tijd voor overleg tussen KMar medewerkers. Het zijn handelingen waarvoor aan de grensdoorlaatpost zelf doorgaans geen tijd of mogelijkheid is.

API-gegevens kunnen ook helpen om passagiers te detecteren en te onderzoeken die niet gesignaleerd staan in de databases maar waar de combinatie van persoons- en vluchtgegevens dermate opvallend is dat het vragen oproept over de intenties van de reiziger. Dat geldt bijvoorbeeld voor een passagier die reist via een niet voor de hand liggende route. Deze passagier kan niet op basis van alleen een controle aan de doorlaatpost worden opgemerkt, maar wel aan de hand van API-gegevens door het API-Centrum.

Hoe API geacht wordt bij te dragen aan bevorderen van de doorstroming

Systematische grenscontrole bij passagiers kost tijd. Het houdt in dat van iedere passagier bij een grensdoorlaatpost het reisdocument moet worden gescand en de gegevens moeten worden vergeleken met SISII, OPS en SLTD. Daarbij moet een grenswachter ook altijd de identiteit van de passagier verifiëren en de geldigheid van het document controleren en in geval van een onderdaan van een derde land eventueel het visum of verblijfsvergunning controleren.

API kan de controle aan de grensdoorlaatposten ontlasten bij aankomende passagiers. Het is ook expliciet benoemd in de wijziging van de Schengengrenscode van 2017[21]. Door de gegevens van een passagier voorafgaand aan diens grenspassage al te vergelijken met de verschillende opsporingsregisters, watchlisten en profielen kan aan de doorlaatpost tijd worden bespaard. In het geval van opsporingsregisters en watchlisten is de persoon en het risico bekend. Er worden verschillende bestanden gebruikt waarmee de API-gegevens worden vergeleken. De vergelijking van gegevens wordt gedaan bij het API-Centrum. Hier wordt voor iedere binnenkomende passagier van buiten het Schengengebied nagegaan of hij voorkomt in SISII of OPS en/of reist met een reisdocument dat als vermist is opgegeven. Tevens wordt nagegaan of er in een combinatie van persoons- en vluchtkenmerken (profielen) een verhoogd risico zit op de kans dat iemand asiel aanvraagt of mogelijk sprake is van illegale immigratie. De grenscontrole wordt hiermee effectiever.

De grenswachter bij de doorlaatpost moet weliswaar nog steeds de identiteit van passagiers vaststellen en verifiëren dat het reisdocument daadwerkelijk hoort bij de persoon, maar hoeft dankzij de screening van het API-Centrum niet iedere passagier te controleren in de systemen. De grenswachter kan gericht uitkijken naar passagiers waarvan reeds een

[21] Artikel 8, lid 2.

alert is vastgesteld. De grenscontrole verloopt hierdoor efficiënter. Hoe dat in de praktijk gebeurt wordt beschreven in hoofdstuk 3.

In de eerdere evaluatie van de API regeling[22] is opgemerkt dat in 2013 het effect van snellere grenspassage nog niet (duidelijk) meetbaar was, vooral vanwege het feit dat de API-verplichting destijds nog niet van toepassing was op alle vluchten van buiten Schengen. Nu is die analyse evenmin duidelijk meetbaar te maken. Er is immers geen vergelijking mogelijk om de situatie zonder API en met API met elkaar te vergelijken en we kunnen niet beschikken over een datareeks waarmee we dit kunnen benaderen. We beperken ons in hoofdstuk 3 daarom tot een kwalitatieve beschrijving.

Een ander verondersteld bijkomend voordeel (los van de verbetering van grenscontroles) is dat de API-verplichting zorgt voor grotere duidelijkheid over wie er aan boord is. Vliegrampen in het recente verleden hebben geleerd dat het lang kan duren voordat er volledige duidelijkheid is over wie er aan boord was. Met de API-verplichting stellen luchtvaart-maatschappijen betrouwbare passagierslijsten samen, waardoor er meer duidelijkheid is over wie er aan boord is gegaan.

2.4 Carrier Liability

Naast de verplichting om API-gegevens en straks (mogelijk) ook PNR-gegevens te verstrekken, hebben vervoerders een zorgplicht ten behoeve van het voorkomen van illegale immigratie. Dit is in Europees verband vastgelegd met de Council Directive 2001/51/EC of 28 June 2001. Deze zorgplicht houdt in dat zij er op toezien dat alle passagiers die zij aan boord nemen op een reis van buiten Schengen naar een Schengenland, in bezit zijn van een geldig reisdocument met daarin eventueel een benodigd visum. De zorgplicht houdt ook in dat vervoerders verplicht zijn passagiers mee terug te nemen aan wie de toegang tot een Schengenland wordt ontzegd. Wanneer de passagier niet meteen mee terug kan worden genomen, moet de vervoerder een alternatieve terugreis verzorgen. In de praktijk komen daar voor de vervoerder dan ook hotelkosten bij. Indien een vervoerder door nalatigheid mensen aan boord heeft genomen zonder geldig reisdocument, kan ook een boete worden opgelegd.

De Carrier Liability zorgt ervoor dat luchtvaartmaatschappijen van al hun passagiers die van buiten het Schengengebied naar Nederland vliegen, in principe het reisdocument hebben gecontroleerd. Dit draagt ertoe bij dat de API-gegevens van passagiers doorgaans een hoge betrouwbaarheid hebben. In dit verband wordt wel gezegd dat API-gegevens gevalideerde gegevens zijn. Dankzij de API gegevens weet de KMar ook met welke maatschappij een passagier is vervoerd en kan daarmee ook deze maatschappij aanspreken.

[22] Evaluatie API, 2013, pag 37

2.5 Actuele Europese ontwikkelingen

Smart Borders
De combinatie van meer passagiers en hogere veiligheidseisen zijn aanleiding geweest om te zoeken naar mogelijkheden om grote passagiersstromen zonder opstoppingen te kunnen afhandelen en daarbij geen concessies te doen aan veiligheidseisen en het respect voor de rechten van passagiers. Het aantal niet-EU passagiers dat van buiten Europa komt groeit en de verwachting is dat deze groei de komende jaren doorzet (van de circa 50 miljoen niet-EU passagiers in 2015 naar 76 miljoen in 2025[23]).

De maatregelen die in Europees verband worden getroffen zijn voortdurend in ontwikkeling. Belangrijke recente ontwikkelingen en maatregelen die onder de noemer Smart Borders vallen, zijn o.a.:

- Entry-Exit System (EES): in november 2017 heeft de Europese Raad bepaald dat er een EES komt. Hiermee worden alle Schengengrensoverschrijdingen van niet-EU ingezetenen geregistreerd.[24] Niet alleen voor inkomende passagiers, ook voor uitgaande passagiers. Zo kan worden gedetecteerd hoe lang niet EU-ingezetenen in het EU-gebied zijn geweest. Een kort verblijf van 90 dagen in het Schengengebied inclusief Zwitserland is toegestaan. Deze controle wordt nu gedaan door de datumstempels in paspoorten te controleren. Dit is een bewerkelijk en foutgevoelig proces.
- ETIAS: de Europese Raad heeft 5 september 2018 een verordening aangenomen die bepaalt dat er een Europees systeem voor reisinformatie en -autorisatie wordt opgezet. Het systeem is vergelijkbaar met het Amerikaanse Electronic System for Travel Authorization (ESTA). Het houdt in dat niet-visumplichtige onderdanen van derde landen voor hun reis naar een Schengenland een reisautorisatie moeten aanvragen.
- Systematische grenscontrole aan de hand van databases: op 7 maart 2017 heeft de Europese Raad een verordening tot wijziging van de Schengengrenscode aangenomen om de controles aan de buitengrenzen aan te scherpen. De lidstaten zullen alle mensen aan de grenzen systematisch moeten controleren aan de hand van relevante databanken.
- Interoperabiliteit: binnen de EU wordt gewerkt aan de verbetering van interoperabiliteit van informatiesystemen, zoals o.a. EES, Visa Information System (VIS), ETIAS en SISII. De bedoeling is dat deze systemen beter op elkaar aansluiten en elkaars gegevens kunnen gebruiken en actualiseren.
- Verbetering van SISII: er worden onder andere nieuwe categorieën van signaleringen aan SISII toegevoegd.

Bij invoering van EES en ETIAS is het mede in het kader van de carrier liability van belang dat luchtvaartmaatschappijen kunnen beoordelen of iemand een ETIAS reisautorisatie heeft en of de 90 dagen termijn niet is overschreden. Derde-landers mogen 90 dagen in een periode van 180

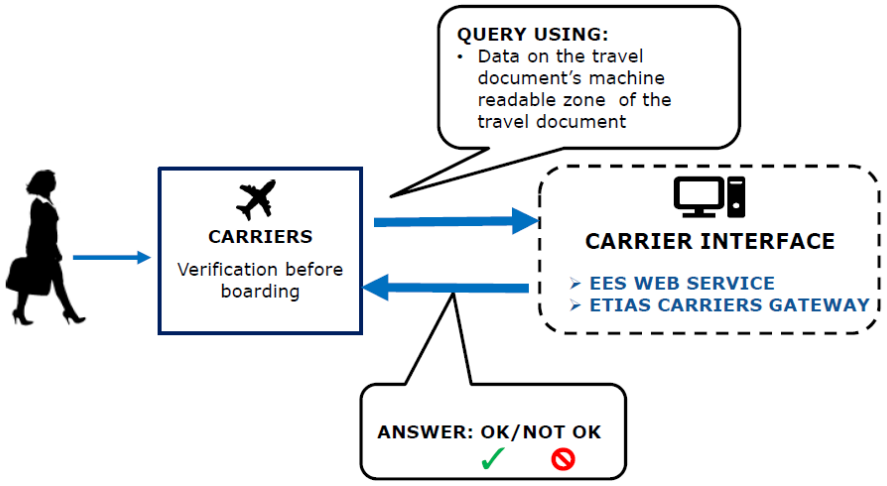
[23] EPRS, Smart Borders: EU Entry/Exit System, 2018 9.12
[24] EU OJ L 327 9.12.2017.

dagen in het Schengengebied verblijven[25]. In figuur 1 is schematisch weergegeven hoe het systeem voor luchtpassagiers gaat werken. De figuur geeft weer hoe de carriers invulling kunnen geven aan hun verplichtingen uit carrier liability na de start van het gebruik van EES/ETIAS.

Vergelijkbare systemen om voor het vertrek aan te geven of passagiers toestemming hebben om te reizen naar het bestemmingsland zijn al in werking in de VS, Canada en Australië. Deze landen vallen uiteraard buiten de reikwijdte van de Europese API richtlijn maar geven mogelijk een richting aan voor de vorm die de EU kan kiezen met betrekking tot de combinatie van gegevens en registers om te beoordelen of passagiers naar de EU mogen reizen.

Luchtvaartmaatschappijen krijgen hierbij voorafgaand aan het boarden per passagier een OK/NOT OK TO BOARD signaal. Maatschappijen krijgen zelf geen toegang tot de persoonsgegevens in de systemen die het OK/NOT OK sturen. Vooralsnog is er van zo'n interactief systeem binnen de EU nog geen sprake. Binnen de EU is met de huidige manier van data-aanlevering interactie nog niet mogelijk. De API-gegevens worden nu via een PAXLST protocol als batch verstuurd. Bij interactieve systemen wordt een reisdocument aan de gate door een lezer gehaald en is interactie nodig met de autoriteiten in het bestemmingsland om na de vergelijking met opsporingsregisters de respons te kunnen geven. In het geval van de EU is het mogelijk dat dit uiteindelijk centraal wordt geregeld voor alle EU-lidstaten. Dit stelt hogere eisen aan de dataverbindingen: als een dataverbinding niet werkt kunnen de passagiers niet aan boord en kan het vliegtuig niet vertrekken.

figuur 1 Schematische weergave Smart Border



Bron: Europese Commissie, 2017

[25] https://www.nederlandenu.nl/reizen-en-wonen/visa-voor-nederland

Passenger Name Record (PNR)
Sinds de aanslagen in Madrid, Londen, Parijs en Brussel krijgt in Europees verband het bestrijden van terrorisme meer aandacht. Eén van de resultaten daarvan is de EU Richtlijn 2016/681

> *'over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit'* (Memorie van Toelichting, Vergaderjaar 2017-2018, 34861; Casagran, 2015).

Waar de API-richtlijn volgt op een mondiaal initiatief, is de PNR-richtlijn een Europees voorstel. Het wetsvoorstel voor de implementatie van deze richtlijn heeft de minister van Justitie en Veiligheid op 9 januari jl. aan de Tweede Kamer aangeboden.

Met deze beoogde wet worden vervoerders verplicht gegevens waarover zij beschikken van hun passagiers te verstrekken aan de op te richten Passenger Information Unit (PIU, voor Nederland: Pi-NL). PNR gegevens worden aangemaakt om een reis te kunnen boeken en komen uit het reserveringssysteem van de luchtvaartmaatschapijen. Als de reis niet direct bij een luchtvaartmaatschappij is geboekt maar via een tussenpersoon, dan is het mogelijk dat de luchtvaartmaatschappij geen of nauwelijks PNR-gegevens heeft. Tussenpersonen (agenten, reisbureaus, touroperators) beschouwen die gegevens namelijk als hun eigendom en verstrekken die liever niet aan de maatschappijen om te voorkomen dat die de passagiers vervolgens direct gaat benaderen.

De doelbinding bij de API-richtlijn is het verbeteren van grenscontroles en het tegengaan van illegale migratie. De doelbinding bij PNR-richtlijn is het bestrijden van ernstige criminaliteit en terroristische misdrijven. Het aantal gegevens in de PNR-dataset is aanzienlijk omvangrijker dan de API-set. In bijlage 4 zijn de datarubrieken en datavelden opgenomen waaruit de PNR-data die in het wetsvoorstel is voorgeschreven is opgebouwd. API-gegevens vormen een subset van deze gegevens.

De Pi-NL heeft tot taak de PNR-gegevens van de luchtvaartmaatschappijen te verzamelen, op te slaan en te verwerken, en die gegevens of het resultaat van de verwerking ervan aan de bevoegde instanties door te geven. Dit zijn het Openbaar Ministerie, de Nationale Politie, de KMar, bijzondere opsporingsdiensten en de Rijksrecherche (MvT, Vergaderjaar 2017-2018, 34861).

De Pi-NL is een zelfstandige eenheid die beheersmatig is ondergebracht bij de Kmar. De Pi NL is echter geen onderdeel van de Kmar. De taken van de Pi-NL maken geen deel uit van de politietaken die aan de KMar zijn opgedragen op grond van artikel 4 van de Politiewet 2012. De KMar als zodanig wordt dus niet de Nederlandse PIU en heeft ook geen toegang tot de systemen van de Pi-NL. Bevoegde instanties kunnen gegevens opvragen en/of ontvangen van de Pi-NL, uiteraard met inachtneming van de wettelijke voorwaarden en verwerkingsdoeleinden.

In de memorie van toelichting van de PNR-wet staat dat voor de KMar geldt dat de verwerking van PNR-gegevens geen betrekking kan hebben op handhaving van de openbare orde of toezichtstaken en daarom ook niet op de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken van de KMar. In de memorie van toelichting wordt dit niet verder toegelicht. De KMar kan wel PNR-gegevens in het kader van de grensbewakingstaak ontvangen van Pi-NL en verwerken ten behoeve van de uitoefening van haar opsporingstaken. De betreffende gegevens moeten daartoe gevorderd worden via het OM. Een dergelijke verwerking kan bijvoorbeeld noodzakelijk zijn wanneer uit een vergelijking van passagiersgegevens met een databank blijkt dat een voortvluchtige verdachte zal aankomen op Schiphol en deze verdachte dient te worden aangehouden of bij een overeenkomst met risico-criteria naar aanleiding waarvan een nadere controle van een passagier door de KMar noodzakelijk is (MvT, Vergaderjaar 2017-2018, 34861). In het PNR-wetsvoorstel wordt een bewaartermijn genoemd van 5 jaar. Passagiersgegevens waaruit rechtstreeks de identiteit van een persoon kan worden afgeleid worden na zes maanden gedepersonaliseerd door afscherming van die gegevens.

Verwerking van PNR-gegevens in het kader van het PNR-wetsvoorstel is uitsluitend toegestaan om terroristische misdrijven en bepaalde vormen van ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen. Wat daaronder concreet wordt verstaan, is ook geïnventariseerd. In bijlage 2 van het wetsvoorstel worden in totaal 26 strafbare feiten benoemd waaronder: mensenhandel, cybercrime en illegale wapenhandel.

De luchtvaartmaatschappijen worden met de PNR-wet verplicht om passagiersgegevens die zij voor hun eigen bedrijfsdoeleinden verzamelen (inclusief de verplichtingen die voortvloeien uit bestaande nationale en internationale regelgeving op het gebied van luchtvaart, immigratie, e.d.) te verstrekken aan Pi-NL. Onder passagiersgegevens worden zowel PNR- als API-gegevens begrepen voor zover deze beschikbaar zijn. In bijlage 4 is een overzicht opgenomen van de API- en PNR-gegevens. Tot de PNR-gegevens behoren onder andere: persoonsgegevens, samenstelling van het reisgezelschap, boekings-gegevens, vluchtgegevens, bagagegegevens, zitplaats in het vliegtuig en betaalgegevens. Indien API-gegevens door luchtvaartmaatschappijen verzameld zijn dan moeten die ook worden aangeleverd bij Pi-NL[26].

Vervoerders hoeven de PNR-gegevens niet te verifiëren. Met andere woorden: een vervoerder hoeft niet in een fysiek één-op-één contact na te gaan of de passagier werkelijk degene is die hij zegt te zijn. Een aantal luchtvaartmaatschappijen voert die controle overigens wel uit. Het NCTV geeft aan dat momenteel de mogelijkheden worden verkend voor invoering van een conformiteitscheck. De doorgifte van de gegevens dient elektronisch plaats te vinden en is in ieder geval verplicht op twee momenten. De eerste keer is verstrekking verplicht op enig moment tussen 48 uur van tevoren en 24 uur voor de geplande vertrektijd van de vlucht en het tweede moment van verstrekking vindt plaats onmiddellijk na het aan boord gaan van de passagiers in het vliegtuig dat klaar staat

[26] Het kan ook zijn dat een vervoerder intra-EU deze gegevens ook verzamelt, dan moeten deze ook meegestuurd worden aan de Pi-NL.

voor vertrek en waarvan de passagiers niet meer van boord kunnen gaan (MvT, Vergaderjaar 2017-2018, 34861). In de praktijk, als de PNR-wet wordt aangenomen conform het huidige wetsvoorstel, is afgesproken dat dit voor Nederland op 3 momenten te laten plaatsvinden: 48 en 24 uur van tevoren en bij vertrek.

Als de PNR-wet wordt aangenomen in de huidige vorm, krijgt de KMar de beschikking over twee typen van data:

- API-datastroom: De KMar mag deze gegevens gebruiken voor de grenscontrole en het tegengaan van illegale immigratie in het kader van de doelbinding van de API richtlijn en de Vreemdelingenwet.
- Het resultaat van de verwerking van PNR data: de KMar krijgt het verwerkingsresultaat van de PNR-gegevens bij Pi-NL voor passagiers die in verband worden gebracht met de opsporing van zware criminaliteit en/of terrorisme. Dit is niet per definitie hetzelfde KMar-loket.

Behoefte aan single window bij luchtvaartmaatschappijen

IATA spreekt nadrukkelijk de wens uit om te werken aan een 'single window' (één loket voor alle transacties) om al deze informatiestromen van passagiersgegevens aan de autoriteiten te faciliteren (IATA position paper 2017). Een 'single window' moet bijdragen aan het beperken van de administratieve belasting van maatschappijen. Op verschillende momenten moeten luchtvaartmaatschappijen data aanleveren. Het gaat dan om API- en PNR-data. IATA heeft de voorkeur om bij de nationale autoriteit van het bestemmingsland alle data aan te leveren op een uniforme manier die voor alle landen in de EU gelijk is. Die wens leeft bij IATA en de aangesloten maatschappijen overigens ook ten aanzien van de huidige verplichtingen rond passagiersinformatie (IATA 2017).
De Nederlandse overheid verkent de mogelijkheden om zo'n single window ook voor Nederland te realiseren.

3 API in de praktijk

3.1 Inleiding

In het voorgaande hoofdstuk is beschreven wat de API-verplichting inhoudt en hoe die samenhangt met andere verplichtingen rond de aanlevering van passagiersinformatie. In dit hoofdstuk wordt ingegaan op hoe de verplichting in de praktijk wordt opgevat, hoe zij een plek heeft gekregen in bedrijfsprocessen en wat de verplichting concreet betekent voor de grenscontrole en het tegengaan van illegale immigratie. Ook beschrijven wij aan de hand van casussen hoe het begrip grenscontrole wordt opgevat en welke gegevens daarvoor in combinatie met de API-gegevens worden gebruikt. Ten behoeve van het overzicht maken we onderscheid tussen de ervaringen van de geïnterviewde luchtvaartmaatschappijen en ervaringen van de geïnterviewde KMar medewerkers.

3.2 Praktijk bij luchtvaartmaatschappijen

In de praktijk van het verzamelen en verwerken van passagiersgegevens ten behoeve van de API-verplichting geldt voor luchtvaartmaatschappijen 'the estimated time of departure' als belangrijk ijkpunt. Rond dat moment moeten de API-gegevens aan de KMar worden verstuurd. Eén van de respondenten merkte hierover op:

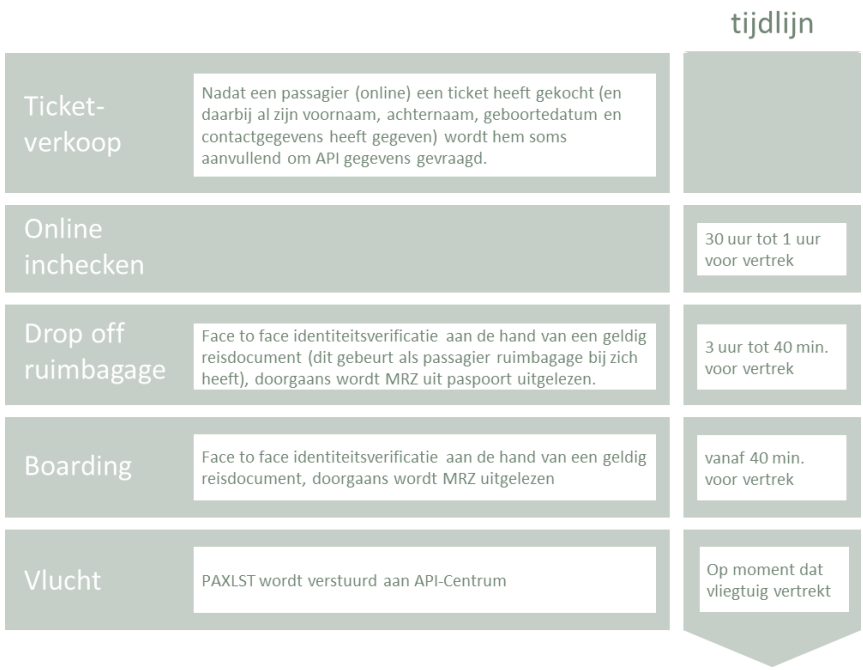
> *'Je wilt de API data niet pas bij het boarden verzamelen, dat is te laat'. 'Bij het boarden moet een vlucht helemaal schoon zijn, het hele proces dat er aan voorafgaat, is zo ingericht dat passagiers die niet mogen reizen er vrijwel allemaal zijn uitgehaald.'*

Dit betekent dat luchtvaartmaatschappijen API-gegevens niet pas bij het boarden vastleggen maar al tijdens het boeken en de check-in. Dit kan de passagier zelf doen via de website of het vindt plaats aan het loket op de luchthaven.

Validatie van de gegevens vindt vervolgens plaats op de luchthaven, tijdens het zogenoemde 'first point of contact'. Tot enkele jaren geleden was het moment van inchecken het eerste contactmoment. Nu is dat moment grotendeels komen te vervallen, omdat steeds meer passagiers online inchecken. Voor vluchten van buiten het Schengengebied is het 'first point of contact' daardoor vaak het moment dat een passagier zijn ruimbagage afgeeft aan de balie. Voor passagiers die geen ruimbagage afgeven, is het eerste contactmoment het moment dat zij aan boord gaan (identiteitsvalidatie aan de gate). Veelal worden gegevens – die in een paspoort zijn opgenomen in de zogeheten Machine Readable Zone (MRZ)[27] – aan de balie en/of de gate digitaal uitgelezen. De gegevens hebben hiermee een hoge betrouwbaarheid.

[27] In de chip die in paspoorten zit opgenomen is een aantal gegevens vastgelegd die machinaal zijn uit te lezen

figuur 2 Handelingen ten behoeve van API-verplichting ten aanzien van de Nederlands autoriteiten voor vluchten die de Schengenbuitengrens passeren.



Het aannemen van ruimbagage hebben luchtvaartmaatschappijen regelmatig uitbesteed. Twee van de drie maatschappijen met wie wij spraken, hebben hun gehele grondafhandeling op al hun bestemmingen uitbesteed. Voor naleving van de API-richtlijn zijn de luchtvaartmaatschappijen eindverantwoordelijk en aanspreekbaar voor de autoriteiten. Alle handelingen die nodig zijn om het toestel met de juiste passagiers en bagage te laten vertrekken, zijn neergelegd bij een 'onderaannemer'. Het valideren van persoonsgegevens behoort tot de taken van de onderaannemers. Luchtvaartmaatschappijen maken zelf afspraken met deze grondafhandelaars over hoe eventuele boetes voor het niet-naleven van de API-verplichting kunnen worden doorbelast als blijkt dat de afhandelaars fouten hebben gemaakt. De maatschappijen zelf blijven eindverantwoordelijk ten opzichte van de autoriteiten.

Vervoerders en hun grondafhandelaars hebben hun systeem zo ingericht dat inchecken of boarden onmogelijk is als API-gegevens ontbreken. Zo staat het systeem het bijvoorbeeld niet toe bagage in te nemen van een passagier van wie het nummer van zijn reisdocument (paspoort) ontbreekt of van een passagier die geen geldig reisdocument kan tonen en tijdens zijn reis een Schengengrens passeert.

Tijdens het proces dat loopt van ticketverkoop tot aan de vlucht, verstrekt een luchtvaartmaatschappij op verschillende momenten passagiersgegevens aan overheden. Door de Nederlandse overheid wordt dat op één moment voorgeschreven. In het Voorschrift Vreemdelingen (art. 2.1a) is bepaald dat een vervoerder vóór beëindiging van de instapcontrole de gegevens verstuurt. In de praktijk gebeurt dit vaak op het moment dat het vliegtuig daadwerkelijk is vertrokken omdat er tussen het tijdstip van boarden en daadwerkelijk vertrek nog veel kan gebeuren. Er kan zich bijvoorbeeld een technische storing voordoen of het krijgen van een timeslot om te vertrekken loopt vertraging op of het weer kan plotseling verslechteren waardoor het vliegtuig later of niet vertrekt.

Er bestaan verschillen tussen landen met betrekking tot de momenten waarop passagiersgegevens moeten worden aangeleverd. De verschillen zijn niet direct relevant voor de Nederlandse API-praktijk, maar geven wel aan hoe luchtvaartmaatschappijen moeten inspelen op de verschillende eisen die er aan hun activiteiten en het voldoen aan de regelgeving worden gesteld. Voor landen met interactieve screening van passagiersgegevens (zie tekstkader) geldt dat zij vervoerders verplichten al 48 uur voor het geplande vertrek inzage te geven in de gegevens. Het interactieve systeem stelt deze landen vervolgens in staat het inchecken of boarden van een passagier te blokkeren op het moment dat deze gesignaleerd staat of niet over het benodigde visum beschikt.

Ook bestaan er verschillen tussen landen in de mate waarin zij geïnformeerd willen worden over vluchten. De Verenigde Staten stellen luchtvaartmaatschappijen ook verplicht om API-gegevens te verstrekken bij vluchten die over haar grondgebied gaan (zonder daar te landen). In de praktijk leidt dit tot omvangrijk dataverkeer. Een luchtvaartmaatschappij illustreerde dat met het volgende voorbeeld:

> *'Van iedere passagier die vanaf Amsterdam via Londen naar Toronto vliegt, moeten de API-gegevens worden verstrekt aan zowel het Verenigd Koninkrijk, de Verenigde Staten als aan Canada. Of een passagier aan deze vlucht kan beginnen hangt daarmee af van de beoordeling van drie verschillende landen.'*

Interactieve screening op basis van passagiersgegevens (o.a. Verenigde Staten)

De Verenigde Staten (VS) hanteert een interactief systeem. De Amerikaanse autoriteiten hebben toegang tot een deel van het boekingssysteem van luchtvaartmaatschappijen en kunnen voorafgaand aan de vlucht bepalen of een passagier mag reizen naar de VS of niet. Een passagier kan pas aan boord wanneer de Amerikaanse autoriteiten daar groen licht voor hebben gegeven. Het systeem heeft zowel tot doel illegale immigratie tegen te gaan als de nationale veiligheid te beschermen. Elke passagier die naar de Verenigde Staten reist, wordt op beide aspecten gescreend en krijgt afhankelijk daarvan een code die bestaat uit een cijfer en een letter. De screening gebeurt vanaf 48 uur voor vertrek.

Het cijfer uit de code verwijst naar het veiligheidsrisico. De letter heeft betrekking op immigratie.

- Cijfer: elke code bevat het cijfer 0,1,2,3 of 4. Waarbij 0 en 1 staan voor een hoog risico en 4 voor een laag risico. Bij een hoog risico wordt een passagier eerst onderzocht, voor hij eventueel toch aan boord gaat. De security officer van de maatschappij kan hiervoor in contact treden met de Amerikaanse autoriteiten.
- Letter: elke code bevat verder de letter A,B,C,D,E,X of Z. Een passagier met A beschikt bijvoorbeeld over de juiste papieren, een passagier met een B heeft geen Esta.

De API-gegevens worden ten behoeve van de Nederlandse grenscontrole ‘gepushed’ naar het API-Centrum; dat wil zeggen dat de luchtvaartmaatschappij de gegevens verstrekt.

Het verstrekken van de gegevens aan de Nederlandse grensautoriteiten gebeurt met een telexbericht, volgens een standaard format (PAXLST), zoals voorgeschreven in het Voorschrift Vreemdelingen (art. 2.1.a). De verstrekking van de gegevens gaat via een broker, een dienstverlener die voor de gegevensuitwisseling zorgdraagt. Het aantal API-velden is in Nederland uitgebreid conform de toezegging van de Minister naar aanleiding van de evaluatie van 2014. Deze uitbreiding helpt de screening van gegevens te verbeteren. We kunnen dit effect echter niet op basis van de beschikbare registraties kwantitatief onderbouwen omdat na 2014 ook veel andere elementen rond API zijn veranderd, waaronder de uitbreiding van het aantal vluchten en verbeteringen in de kwaliteit van de registers.

Hoewel dit rapport zich beperkt tot een evaluatie van de Nederlandse regelgeving naar het gebruik van API gegevens, hebben andere overheden en dan met name die van de Amerikaanse overheid, een grote invloed op hoe in de sector de verplichtingen rond het verzamelen en verstrekken van passagiersgegevens worden ervaren.

Luchtvaartmaatschappijen zijn inmiddels voorbereid of al ingesteld op het aanleveren van meer data dan alleen API als het PNR-wetsvoorstel wordt aangenomen. De vergelijking die luchtvaartmaatschappijen maken met het Amerikaanse systeem verklaart dat de strikte scheiding tussen PNR en API in de huidige Nederlandse praktijk vragen oproept bij luchtvaartmaatschappijen over de strikt gescheiden aanlevering en gebruik van passagiersgegevens. Die keuze is bij de invoering van API destijds in Nederland gemaakt. Respondenten van luchtvaart-maatschappijen zien het Amerikaanse single window dat is ingericht door de Transport Security Administration (onderdeel van het Department of Homeland Security) als wenselijk voorbeeld. Bij voorkeur zelfs één loket voor alle Europese lidstaten, maar in ieder geval één loket per land. Tevens wordt verwezen naar bijvoorbeeld SITA. SITA[28] is een private partij die een single window functie vervult in het API-verkeer tussen luchtvaartmaatschappijen en een groep van landen waaronder Zuid Afrika, Thailand en de Verenigde Arabische Emiraten. SITA verzorgt dus niet alleen het dataverkeer maar ook de distributie van de gegevens aan de autoriteiten van de verschillende landen. In Nederland wordt nu ook gewerkt aan de invoering van een 'single window'.

Naleving

De ervaringen met het aanleveren van API-gegevens en het contact daarover met de KMar zijn over het algemeen positief. Het versturen van de API-bestanden is onderdeel van de routine. KMar spreekt van een '100% compliance' op alle routes waarop de API-verplichtingen van toepassing zijn. Het beeld dat uit de gesprekken naar voren komt, is dat het op een enkele vlucht na altijd goed gaat. Over de gevallen waarin het niet goed gaat, is altijd adequaat overleg met de KMar. *'Het contact met de KMar is buitengewoon prettig, we weten elkaar goed te vinden',* aldus een respondent van één van de maatschappijen. Hierbij moet worden opgemerkt dat in het kader van dit onderzoek alleen is gesproken met drie Nederlandse luchtvaartmaatschappijen.

Het zijn met name twee situaties waarin het voorkomt dat API-data niet zijn verstuurd en de KMar aanleiding ziet om contact op te nemen:

- Vluchten die zijn gecanceld: het komt voor dat de KMar API-data verwacht van een vlucht die gecanceld blijkt te zijn.
- Vluchten aan het begin van een seizoen: de frequentie waarmee luchtvaartmaatschappijen op bepaalde bestemmingen vliegen, kan per seizoen verschillen. Als op een bepaalde bestemming het seizoen weer start, komt het incidenteel voor dat bij de eerste vlucht vergeten wordt de API-gegevens te versturen.

Er zijn voor zover bekend bij de KMar en de bevraagde luchtvaartmaatschappijen geen boetes opgelegd vanwege het niet nakomen van de API-verplichting. Tot nu toe worden geconstateerde lacunes altijd wel gemeld en besproken maar nooit beboet. Er zijn wel officiële waarschuwingen uitgegaan.

[28] https://www.sita.aero/

Een aspect van de API-richtlijn waarvan de naleving aandacht behoeft, is de verplichting voor luchtvaartmaatschappijen om de verstrekte persoonsgegevens (API-gegevens) te vernietigen. De Europese API-richtlijn bevat daarover de volgende bepaling*:*

> *'De lidstaten nemen de nodige maatregelen om de vervoerders te verplichten binnen 24 uur na aankomst van het vervoermiddel overeenkomstig artikel 3, lid 1, de in het kader van deze richtlijn door hen verzamelde en aan de grensautoriteiten verstrekte persoonsgegevens te vernietigen'* (Richtlijn 2004/82/EG van de Raad, 29 april 2004).

In de gesprekken is op het onderdeel bewaringstermijn meerdere keren verwezen naar de Wet bescherming persoonsgegevens, die inmiddels is vervangen door de Algemene Verordening Gegevensbescherming (AVG), die een langere bewaartermijn toestaat. Voor de geïnterviewde luchtvaartmaatschappijen geldt dat ze hun reserveringsgegevens in ieder geval wel langer dan 24 uur bewaren. Reserveringsgegevens zijn niet gelijk aan API-gegevens. Er is echter wel overlap met de API-data. De KMar kan overigens in bepaalde omstandigheden data 36 uur bewaren. Dit is het geval bij derdelanders waarbij sprake is van een risico op illegale immigratie. Onder de Wet politiegegevens (Wpg) kan de bewaartermijn zelfs oplopen tot 5 jaar.

Kosten voor luchtvaartmaatschappijen

Geen van de luchtvaartmaatschappijen was in staat om in het gesprek een overzicht te geven van de kosten die zij maken ten behoeve van de API-verplichting. Dat komt vooral omdat de handelingen die nodig zijn voor het verwerken van API-gegevens, vergaand zijn ingebed in de overige bedrijfsprocessen en boekingssystemen. De maatschappijen die wij hebben gesproken gebruiken voor de verwerking van hun boekingen software (zoals 'Amadeus' en 'Go Now') waarin de verwerking van API-gegevens is geïntegreerd. Verder geldt dat de belasting die uitgaat van de API-verplichting, voor een belangrijk deel terechtkomt bij de grondafhandelaars. Een luchtvaartmaatschappij*:*

> *'Het is voor onze agents <grondafhandelaars> best veel, al die landen met andere voorschriften en alle systemen waarmee gewerkt wordt. Zij werken met verschillende instructies waarin tot op detail is beschreven wat er moet gebeuren in welke gevallen'*.

Verder komt uit de gesprekken naar voren dat de kosten van de API-verplichting hoger zijn naarmate de maatschappij vanaf meer verschillende locaties buiten Schengen vliegt. Voor een klein deel gaat het om de kosten die verband houden met de data-aanlevering. Bij meer vluchten van buiten Schengen is de kans groter op vragen van de KMar die opgehelderd moeten worden. Bijvoorbeeld over gegevens die niet zijn ontvangen terwijl de KMar wel gegevens volgens de vluchtplanning verwacht. De luchtvaartmaatschappij moet dan controleren of de vlucht ook daadwerkelijk is vertrokken of dat er iets anders aan de hand is. Zo komt het incidenteel voor dat ondanks het geautomatiseerde proces een PAXLST niet wordt verstuurd en vervolgens op verzoek van KMar moet worden nagegaan waarom niet. Daarnaast zijn er ook op hoger niveau issues die aandacht vragen zoals verzoeken van andere overheden om

gegevens die conflicteren met Nederlandse wetgeving met betrekking tot de verwerking van persoonsgegevens. Een voorbeeld daarvan is de Mexicaanse overheid die de API-gegevens aangevuld wilde zien met de geboorteplaats van de passagier. Tegenover de wens van de Mexicaanse overheid stond een verbod van de Nederlandse Autoriteit Persoonsgegevens.

Eén van de grote maatschappijen die wij spraken, participeert ook actief in overleg over API in IATA verband om de belangen van de sector op dit dossier te behartigen.

Kosten verzenden PAXLST
Een onderdeel van de API-verplichting waarvan de kosten wél eenduidig kunnen worden onderscheiden, betreft het telexverkeer. API-gegevens worden per vlucht op één moment aan de KMar verstrekt. De kosten daarvan zijn variabel en bedragen één duizendste eurocent per karakter. Per passagier gaat het om zo'n 500 karakters (persoon- en vluchtgegevens). Op een vlucht met 190 passagiers komen de kosten voor de luchtvaartmaatschappij per telex daarmee uit op circa 50 eurocent.

In de gesprekken die voor deze studie zijn gevoerd over de manier en momenten waarop API-gegevens worden verstrekt, gingen maatschappijen vaak ook in op PNR-data. Enkele landen (waaronder de Verenigde Staten) stellen maatschappijen al langer verplicht ook deze data (o.a. boekingsgegevens) aan te leveren. In Nederland doet de Douane dat ook sinds 2016 voor het toezicht op de reizigersbagage. Dat gebeurt op vastgestelde tijdslots. Deze tijdslots strekken zich uit tot enkele dagen voordat een passagier vliegt. Met de PNR-wet wordt dat (mogelijk) straks ook in Nederland voorgeschreven en moeten vervoerders in de praktijk op drie momenten de boekingsgegevens (PNR-data) verstrekken: 48 en 24 uur voor de geplande vertrektijd van de vlucht, en onmiddellijk na het aan boord gaan van de passagiers.

Suggesties voor verbetering
De verplichtingen die voortvloeien uit de API-richtlijn zijn ingebed in de bedrijfsprocessen en onderdeel zijn geworden van de bedrijfsroutine. Bij luchtvaartmaatschappijen is minder transparant wat er de verschillen in de (beleidsmatige) context van API en PNR zijn en hoe de grensautoriteiten verder omgaan met de data. Hierbij speelt mee dat maatschappijen met veel verschillende landen te maken hebben en dat deze landen er verschillende doelbindingen op na houden en ook van elkaar verschillen in de mate waarin zij het verzamelen van API- en PNR-gegevens hebben geïntegreerd en ook welke velden zij opvragen. Eerder is al geconstateerd dat de verschillende doelbindingen leiden tot onduidelijkheid en een gebrek aan transparantie (Brouwer, 2017; Sietsma, 2007).

De Amerikaanse grensautoriteiten – waaraan vaak wordt gerefereerd door de drie geïnterviewde luchtvaartmaatschappijen– hebben al toegang tot API-gegevens vanaf 48 uur voor vertrek. Dit betekent dat zij de API-gegevens al kunnen inzien voordat een passagier zich op een luchthaven identificeert. De API-gegevens zijn op dat moment nog niet gevalideerd en onderscheiden zich daarmee minder duidelijk van PNR-gegevens (beide sets zijn immers tijdens de boeking door passagier zelf verstrekt en vertonen bovendien overlap).

De luchtvaartmaatschappijen zijn op de hoogte van de op handen zijnde PNR-wet. De gegevens die een luchtvaartmaatschappij in het kader van deze wet moet gaan verstrekken, hebben in de praktijk overlap met de set van API-gegevens (zie ook bijlage 4). Luchtvaartmaatschappijen worden met het PNR-wetsvoorstel immers geacht per passagier gegevens over reisdocumenten (API-gegevens) te verschaffen als ze die in hun bezit hebben. Die verplichting geldt in het wetsvoorstel dan ook voor passagiers die binnen het Schengengebied reizen. Eén van de respondenten merkte in dit kader op:

> *'Binnenkort moeten wij ook API-gegevens aanleveren voor alle vluchten binnen Schengen'*.

Het wetsvoorstel geeft aan dat als luchtvaartmaatschappijen passagiersgegevens (PNR en API indien aanwezig) verzamelen intra-EU, dan moeten zij die verzamelde gegevens straks ook aan Pi-NL aanleveren als PNR. Op basis van de PNR-wet worden alle data, ook het API-deel, als PNR-data behandeld. Dus binnen de PNR-doelbinding en met de binnen de PNR-wet vastgelegde bewaartermijnen.

In het verlengde van de onduidelijkheid over de context van API wordt niet goed begrepen waarom in de ontvangst en verwerking van gegevens door de Nederlandse autoriteiten met twee portalen wordt gewerkt: het TRIP voor PNR, en het API-Centrum voor API. Het soort analyses en screening dat op deze data wordt uitgevoerd verschilt nauwelijks. De verschillende autoriteiten maken allemaal gebruik van registers als OPS, SIS en de watchlist. Ze gebruiken ook allemaal profielen. Zoals eerder aangegeven wordt door luchtvaartmaatschappijen vaak gerefereerd aan de Amerikaanse Transport Security Administration die zowel API- als PNR-gegevens verwerkt.

De verwachting, en zeker bij de luchtvaartmaatschappijen ook de wens, is dat op de langere termijn 1 loket 'a single window' voor het aanleveren van passagiersgegevens een wereldwijd toegepast model wordt. In verschillende landen is dat nu al het geval. In Nederland is volgens woordvoerders van NCTV het streven ook 1 loket te realiseren.

De API-richtlijn is in Nederland in 2007 opgenomen in de Vreemdelingenwet. Daarmee zijn in de Vreemdelingenwet ook bepalingen opgenomen die van toepassing zijn op Nederlanders en EU-ingezetenen. Voor alle passagiers en de bemanningsleden moeten immers de API-gegevens worden aangeleverd. Op dit moment worden er al PNR-gegevens aangeleverd via TRIP ten behoeve van de Douane. Gezien de ontwikkelingen op Europees niveau met de PNR-richtlijn en de

Smart Borders plannen is het in Nederland inbedden van de API- en PNR-verplichtingen in één kaderwet rond passagiersgegevens in de burgerluchtvaart in onze ogen een logische route.

3.3 Verwerking en gebruik door Koninklijke Marechaussee

Ontvangst en verwerking API-gegevens door API-Centrum
API-gegevens van de passagiers en de bemanning die door luchtvaartmaatschappijen zijn verzameld en geverifieerd, worden bij vertrek van iedere vlucht verstuurd aan het API-Centrum. Nederland volgt hiermee de aanbeveling op die door ICAO is gedaan om een portaal op te richten waar luchtvaartmaatschappijen centraal hun gegevens kunnen aanleveren. Voor de ontvangst van de data maakt het API-Centrum gebruik van ARINC/Rockwell Collins, een broker, die ervoor zorgt dat de ruwe data (PAXLST) van de luchtvaartmaatschappijen worden geconverteerd naar een bestand dat bruikbaar is voor verwerking door het API-Centrum.

Het API-Centrum vergelijkt de gegevens vervolgens met, opsporingsregisters, watchlists en profielen en kijkt verder naar passagiers met ongebruikelijke combinaties van persoons- en vluchtkenmerken die zouden kunnen wijzen op irreguliere migratie. De aanpak van het API-Centrum 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.

Er worden vier typen van matching onderscheiden:

Directe match: het betreffen passagiers die gesignaleerd staan in SISII, OPS en de watchlists. Men spreekt ook wel van de categorie 'known persons with known risks'. Men zoekt naar specifieke personen die vanwege een specifieke reden staan gesignaleerd. Het zoeken naar deze passagiers gebeurt geautomatiseerd met behulp van een zoekmachine. Deze zoekmachine heeft ruime mogelijkheden om bij het matchen rekening te houden met bijvoorbeeld spelfouten, typefouten in persoonsnamen en met de verschillende notaties/formats (R. van Beek, kan bijvoorbeeld ook worden herkend als R. Beek van) en het wel of niet gebruiken van voorloopnullen in cijfercombinatie. Hiermee kan worden voorkomen dat bij het matchen personen over hoofd worden gezien omdat hun naam in één van de bestanden anders is gespeld. Het belang om dat te voorkomen is met name groot bij personen die staan geregistreerd vanwege hoge veiligheidsrisico's. Op zware delicten wordt daarom ruimer gezocht en eventueel ook gezocht op fonetische namen. Dergelijke ruime matching levert doorgaans meer matches op die door een medewerker van het API-Centrum handmatig worden gecontroleerd. Het komt op bepaalde vluchten voor dat op deze manier 20 matches worden gevonden terwijl het om 1 passagier gaat.

Aanvullende match: een directe match kan aanleiding zijn om na te gaan of er nog andere passagiers mee in verband staan. Dat kan bijvoorbeeld gebeuren op het moment dat er een match is op een passagier die gesignaleerd staat vanwege mensensmokkel. Het API-Centrum kijkt dan of betrokkene samen reist met anderen. Dit gebeurt naast het beoordelen van vliegroutes en bestemmingen ook door gebruik te maken van het PNR-locator nummer te gebruiken (onderdeel van de API-set[29] die Nederland opvraagt). Aan de hand van het PNR-locator number[30] kan worden vastgesteld welke passagiers samen reizen. Hiermee kunnen passagiers naar voren komen die weliswaar zelf niet staan gesignaleerd maar samen reizen met iemand die wel staat gesignaleerd en waarvan het van belang is om aanvullende vragen te stellen aan de grens.

Casus 1: gebruik van PNR locator number
Een persoon uit een visumplichtig derde land reist van buiten Schengen naar Amsterdam. De persoon wordt gesignaleerd omdat betrokkene geen Schengenvisum heeft. Eerder is betrokkene een visum door een Schengenland geweigerd. Aan de hand van het PNR locator number (onderdeel van de API-dataset) constateert het API-Centrum dat de man samen reist met drie Nederlanders. Het kan erop duiden dat Nederland de eindbestemming is.
Het API-Centrum verstuurt een alert met hoge prioriteit met als doel de man enkele vragen te stellen over bestemming, doel van het verblijf, duur en middelen[31].

Match op basis van profiel: het API-Centrum controleert de API-data op passagiers met bepaalde combinaties van persoons- en vluchtkenmerken. Het gaat om combinaties die eerder bij grenscontroles zijn opgevallen bij mensen die onrechtmatig de grens wilden passeren. Deze categorie van matches wordt ook wel aangeduid als die van 'unknown persons with a known risk'. Men zoekt naar passagiers die voldoen aan een combinatie van kenmerken. Het gaat hierbij overigens niet alleen om passagiers die zich mogelijk schuldig maken aan een overtreding van een wet: de matching moet ook helpen bij het detecteren van slachtoffers van (grensgerelateerde) criminaliteit. Bijvoorbeeld mensen die slachtoffer zijn van mensenhandel en onder valse voorwendselen een baan of perspectief is geboden in een voor hen vreemd land. Een voorbeeld daarvan is gegeven in casus 5. Profielen worden bij de KMar samengesteld door de Sectie Analyse en Onderzoek en komen ook tot stand naar aanleiding van het periodieke API-overleg met de Brigade Grensbewakingen en de Brigade Vreemdelingenzaken. Profielen worden met regelmaat bekeken of zij nog voldoen aan het doel en of zij aangepast moeten worden.

[29] Zie: Besluit van 20 december 2012, houdende wijziging van het Vreemdelingenbesluit 2000 in verband met de uitbreiding van de vooraf door de luchtvervoerder te verstrekken passagiersgegevens (standaard API-set).
[30] Dit is het nummer waarmee de boeking is geregistreerd. Onder 1 boeking kunnen meerdere passagiers vallen.
[31] Tijdens het interview met een medewerker van DGC kon niet worden vastgesteld of deze melding is opgevolgd door een gatecontrole.

Handmatige beoordeling: deze beoordeling vindt plaats naast de geautomatiseerde matches op watchlists en profielen. Bij een handmatige beoordeling worden voor bepaalde vluchten de passagiersgegevens integraal bekeken, zonder dat men daarbij vooraf een concreet risico voor ogen heeft. Deze manier van zoeken noemt het API-Centrum ook wel: 'looking for an unknown person with an unknown risk'. Bij deze handmatige beoordeling is men alert op opvallende danwel ongebruikelijke combinaties van persoons- en vluchtgegevens. Passagiers op een vlucht kunnen bijvoorbeeld opvallen vanwege een combinatie van hun nationaliteit, een bijzondere reisroute en vanwege het gezelschap waarin zij reizen en de reisroute van leden van dat gezelschap. Ze kunnen ook opvallen omdat mensen halverwege uit het gezelschap in- of uitstappen.

Indien er sprake is van een (gevalideerde) match tussen een passagier/reisdocument en de genoemde registers en het daadwerkelijk een hit wordt, dan kan de KMar daarop acteren. De KMar doet dat met het uitzetten van een interventiebericht naar de grensdoorlaatposten en DGC: een alert. Dit betekent overigens niet altijd dat een passagier op basis van een alert geweigerd of aangehouden kan worden. Dat geldt bijvoorbeeld voor passagiers die boetes hebben uitstaan. Zij kunnen daar op worden aangesproken, hen kan ook worden verzocht de boete te betalen, maar hen kan niet de toegang tot het land worden ontzegd. De toegang kan wel worden ontzegd aan bijvoorbeeld een derdelander die een gevaar vormt voor de openbare orde en veiligheid. Er kan ook sprake zijn van een onterechte alert. Het kan toch gaan om een andere persoon of er blijkt niets aan de hand te zijn.

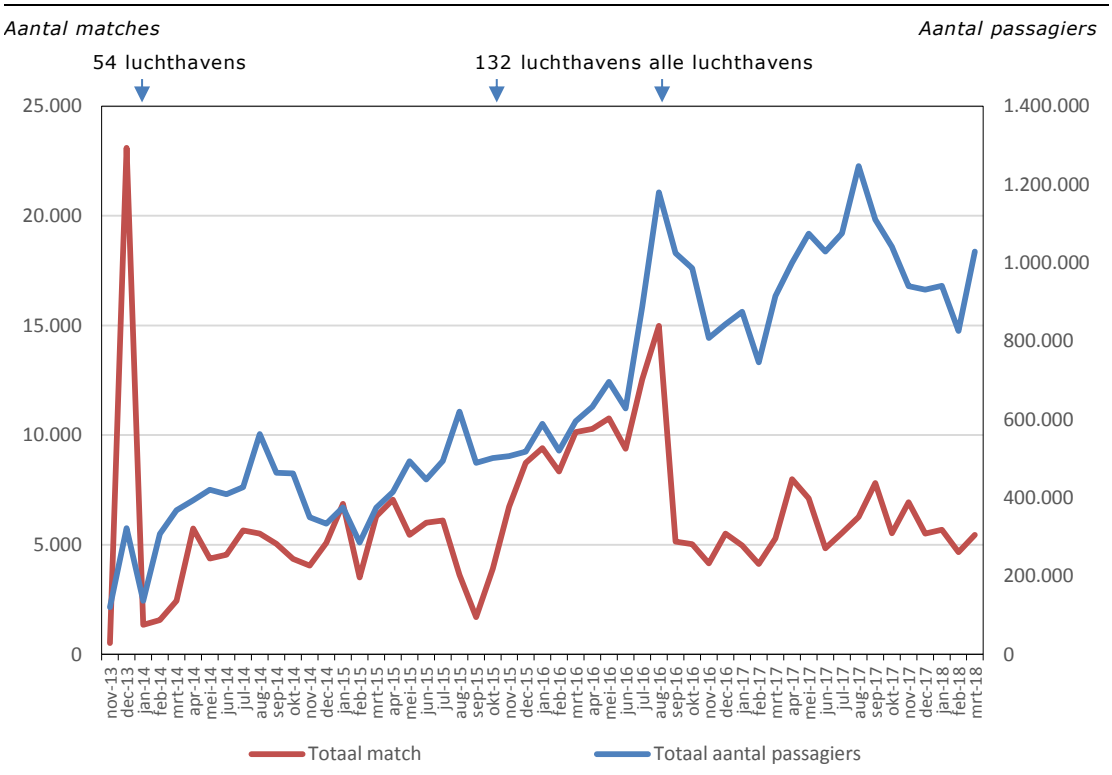
In het kader van de grenscontrole mogen twee autoriteiten de KMar opdracht geven de KMar passagiers te laten signaleren: de Immigratie- en Naturalisatiedienst (IND) en de Nationale Politie. Op Schiphol heeft de KMar ook de politietaak. De IND kan bijvoorbeeld ter ondersteuning van de afhandeling van asielaanvragen de KMar laten uitkijken naar mensen die asiel aan hebben gevraagd, bijvoorbeeld om na te gaan of zij tussentijds terugreizen naar het land van herkomst. De Nationale Politie kan de KMar bijvoorbeeld laten uitkijken naar mensen die in verband worden gebracht met mensenhandel of terrorisme. Hierbij geldt wel dat het Openbaar Ministerie erop toeziet dat dat gebeurt binnen de doelbinding. De Nationale Politie kan de KMar bijvoorbeeld niet laten uitkijken naar mensen die in verband worden gebracht met drugshandel. Dit laatste neemt overigens niet weg dat drugscriminelen wél op basis van een signalering in OPS of SISII kunnen worden aangehouden.

In figuur 3 is een overzicht opgenomen van de ontwikkeling van het aantal matches sinds november 2013. Deze ontwikkeling is afgezet tegen de ontwikkeling van het aantal passagiers. Het gaat hier om passagiers die van buiten het Schengengebied op een Nederlandse luchthaven aankomen. Het aantal passagiers waarvan API-data is verwerkt is in deze periode aanzienlijk gestegen van circa 200.000 per maand naar ruim 1 miljoen. Dit heeft te maken met de uitbreiding van het aantal luchthavens van 54 naar alle niet-Schengenluchthavens én de

groei in de passagiersstromen. Het aantal matches is nauwelijks veranderd. Dat het aantal matches stabiel is kan een gevolg zijn van verbeterde watchlists en profielen. Het aantal matches is volgens de KMar kwalitatief toegenomen. De 'pieken' in de figuur bij het aantal passagiers treden op in de zomermaanden juli-augustus-september. In de figuur is aangegeven voor hoeveel luchthavens de verplichtingen van toepassing waren.

In december 2013 is een piek te zien bij het aantal matches. Dit is een gevolg van het verkeerd invoeren van een profiel. Daardoor zijn veel matches opgetreden die bij verder onderzoek zijn te kwalificeren als false positives. Het aantal matches in de periode 2013-september 2016 verloopt grillig. In de maanden daarna tot en met de laatste gegevens van maart 2018 is een stabilisering te zien. Een verklaring voor deze ontwikkeling is gelegen in de verbeteringen die in de afgelopen jaren zijn gerealiseerd in de verschillende opsporingsregisters en watchlists. Daarnaast is inmiddels veel ervaring opgedaan met het werken aan en met profielen om passagiers met een verhoogd risico op illegale immigratie te detecteren. In de periode vanaf januari 2017 tot en met maart 2018 schommelt het aantal matches tussen de 4.500 en 8.000. De schommelingen in het aantal reizigers spelen hierbij een grote rol.

figuur 3 Aantal passagiers per maand en aantal matches



Bron: KMar

Elke match wordt nagelopen (gevalideerd) door een medewerker van het API-Centrum. Dit is bijvoorbeeld nodig voor matches waarin de zoekmachine ook gelijkende namen heeft opgenomen, zoals eerder in deze paragraaf beschreven onder Directe match. Ook wordt gekeken

naar de actualiteit van signalering en worden eventuele aanvullende gegevens betrokken zoals bijvoorbeeld bejegeningsgegevens uit SISII. Bejegeningsgegevens hebben betrekking op eventuele bijzonderheden van een betrokken persoon, zoals agressiviteit, drugsgebruik of wapenbezit. Op die manier kunnen de KMar-medewerkers aan de gate of balie zich goed voorbereiden op de benodigde actie. Dit draagt ook bij aan de veiligheid van deze KMar-medewerkers.

Wanneer een match is gevalideerd, spreekt het API-Centrum van een 'hit'. Voor elke hit wordt bekeken of een interventie gewenst is. Bij deze beoordeling hanteert het API-Centrum het vier-ogen-principe: het betekent dat er in principe altijd twee mensen betrokken zijn bij de beoordeling van een hit. Wanneer na deze check (extra) controle van de betreffende passagier opportuun wordt geacht, wordt er een interventiebericht opgesteld: een API-alert. API-alerts worden handmatig opgesteld en via de e-mail verstuurd.

Een alert bevat de volgende gegevens:

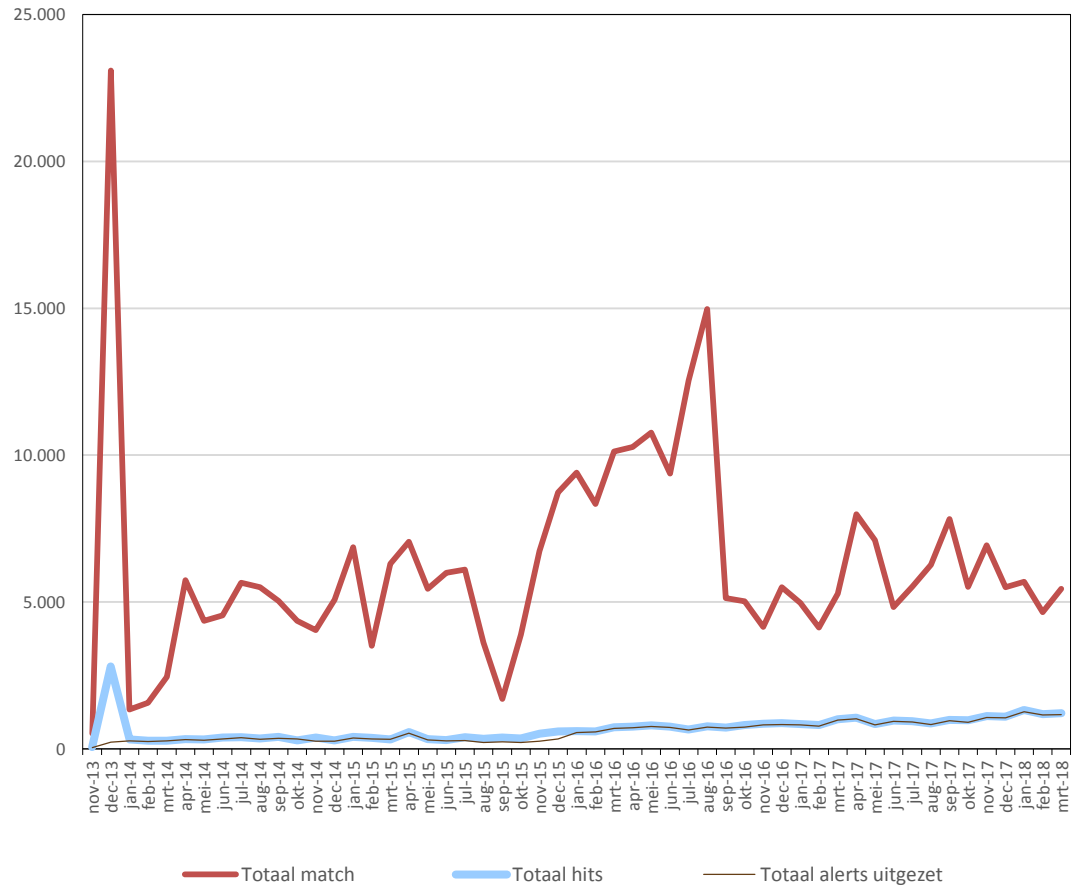
- Enkele API-gegevens zoals volledige naam, geslacht, geboortedatum en vluchtnummer.
- Alert-ID: referentienummer van de alert.
- Beschrijving: in dit veld is aangegeven waarom een persoon staat gesignaleerd. Bijvoorbeeld omdat hij voortvluchtig is, DNA moet afstaan, een boete vanwege een onherroepelijke strafrechtelijke veroordeling moet voldoen, als vermist staat geregistreerd.
- De interventie: bijvoorbeeld aanhouden, in detentie nemen, terugbrengen, onopvallend observeren.
- Opmerkingen: vrij invulveld.
- Openstaande boetes: indien de passagier boetes heeft openstaan, worden die in dit veld getoond. Het gaat om zowel boetes die verband houden met overtredingen, als boetes die verband houden met misdrijven.

In figuur 4 is de verhouding te zien tussen matches, hits en uitgezette alerts. De effecten van een foutieve profielinvoer van december 2013 zijn hier zeer duidelijk te zien. Dit is een evidente uitbijter geweest. Er zijn daardoor ook meer hits gesignaleerd, maar uiteindelijk niet meer alerts uitgezet. Tijdens het valideren zijn de gevolgen van de foute profielinvoer gecorrigeerd. Bij 'Directe match' is hiervoor beschreven dat er bij de screening rekening wordt gehouden met onder andere typefouten, verschillende manieren om een naam of nummer (met voorloopnullen) te noteren en spellingvarianten en dat daardoor het aantal matches in eerste instantie heel groot kan zijn om zo te voorkomen dat de passagier waarom het gaat wordt gemist.

Het aantal alerts loopt vanaf 2013 langzaam op. In november 2017 is voor het eerst sprake van meer dan 1.000 alerts, in de eerste 3 maanden van 2018 gaat het om circa 1.200 alerts per maand.

Met uitzondering van december 2013 worden vrijwel alle hits omgezet in een alert.

figuur 4 Aantal matches, hits en uitgezette alerts



Bron: KMar

In tabel 5 zijn de 10 meest voorkomende redenen voor een alert voor het jaar 2017 opgenomen. Deze top-10 dekt 89% van alle alerts af. Hierbij moet worden opgemerkt dat er meerdere redenen achter één alert kunnen zitten. Een alert kan bijvoorbeeld betrekking hebben op een passagier die zowel gesignaleerd staat vanwege een strafrechtelijk onderzoek als vanwege een boete (Mulderfeit) die nog niet is voldaan. De cijfers laten zien dat het incidenteel voorkomt dat alerts meerdere redenen omvatten. De meeste alerts hebben het Nederlandse OPS als bron en hebben daarmee ook betrekking op in Nederland geregistreerde zaken.

Een aantal alerts is in dit rapport als casus is beschreven om te illustreren hoe met alerts in de praktijk wordt gewerkt. Wat opvalt is dat voor circa 82% wordt gealerteerd naar aanleiding van directe matches.

tabel 5 Top 10 van meest voorkomende alerts in 2017*

		n	% van het totaal aantal alerts
1	Mulderfeit (OPS)	4.164	38%
2	Alert op basis van handmatige beoordeling	1.672	15%
3	Document gesignaleerd als gestolen/vermist (NDS paspoort)	1.515	14%
4	Onopvallende controle (SIS)	449	4%
5	Opsporen aanhouden (OPS)	382	3%
6	Opsporen verblijfplaats (OPS)	365	3%
7	Niet tot Schengengebied toe te laten vreemdeling (SIS)	356	3%
8	Alert op basis van profielen	342	3%
9	Niet onherroepelijk vonnis (vonnis overhandigen met nog een mogelijkheid op een beroepsprocedure binnen een bepaalde termijn) (OPS)	299	3%
10	Betekenis in persoon (uitreiken dagvaarding) (OPS)	283	3%

Bron: KMar

** Tussen haakjes het bestand op basis waarvan de alert tot stand is gekomen*

Het aantal alerts waarbij het gaat om een niet tot het Schengengebied toe te laten persoon is in de periode 2014 tot 2017 duidelijk gestegen van 111 naar 356. Bij deze stijging hoort de kanttekening dat pas vanaf juni 2016 vanaf alle luchthavens van vertrek buiten Schengen API-gegevens worden aangeleverd. Bovendien is de kwaliteit van de internationale registers (SIS) volgens de KMar vanaf 2014 steeds beter en actueler. Op basis van OPS en de watchlist zijn er nog 65 alerts die verband houden met het niet toelaten van personen. Samen telt dit op tot 421 niet toe te laten personen in 2017. In 2018 is in het eerste kwartaal al sprake van 187 alerts rond niet toe te laten vreemdelingen.

De watchlist is een belangrijke toevoeging op OPS en SIS. De watchlist levert vooral alerts op die verband houden met illegale immigratie. In 2017 zijn 49 'contraterrorisme subjects' op basis van de watchlist gealerteerd. In 2016 waren het er 43 en in het eerste kwartaal van 2018 22. Vanaf 2016 zijn er 8 vreemdelingen met een ernstig vermoeden van oorlogsmisdaden in de alerts geregistreerd. De watchlist is hiermee een duidelijke aanvulling op OPS en SIS.

Het totaal aantal alerts dat betrekking heeft op illegale immigratie komt in 2017 uit op 421. Het aantal toegangsweigeringen naar aanleiding van alerts komt op jaarbasis in 2016 en 2017 uit op circa 120 mensen blijkt uit de geregistreerde terugkoppelingen.

Het aandeel van alerts dat voortkomt uit handmatige beoordeling en het gebruik van profielen, ofwel het aantal alerts dat betrekking heeft op 'unknown persons with an unknown risk', komt uit op circa 18%. Het API-Centrum wil stappen zetten om deze handmatige beoordeling verder te ontwikkelen. TCB wil de 'filtersets' die de afzonderlijke medewerkers toepassen, vastleggen zodat zij onderling uitwisselbaar zijn en het gebruik ervan minder afhankelijk is van de aanwezigheid van een specifieke medewerker. TCB spreekt ook wel van de wens om te komen tot het 'product semi geautomatiseerde handmatige beoordeling'.

Verder blijkt dat in 2017 van de in totaal 11.082 alerts 38% betrekking had op een Mulderfeit. De alert heeft betrekking op een bestuurlijke boete waaraan ondanks herhaalde aanmaning niet is voldaan.

Het verder automatiseren van de matching is complex en nu nog niet aan de orde. Hiervoor zijn volgens de KMar drie oorzaken:

- Complexiteit door dynamiek in reispatronen: geautomatiseerde matching houdt in dat voor iedere passagier de positie bepaald wordt ten opzichte van een standaardnormaalverdeling. Dit is complex: afgezien van het gegeven dat hierin verschillende variabelen moeten worden meegenomen, is er sprake van een grote dynamiek. Passagierspatronen veranderen voortdurend. Wat vorig jaar uitzonderlijk was, hoeft dat dit jaar niet meer te zijn. Een land waar eerder nauwelijks passagiers vandaan kwamen, kan opeens sterk opkomen, bijvoorbeeld omdat het zich heeft ontwikkeld tot transitpunt. Dit gold recent voor een aantal landen in het Midden-Oosten. Profielen moeten daarom voortdurend mee veranderen. De complexiteit en dynamiek vereist volgens de geïnterviewden dat modelbouw meer capaciteit (kwantitatief en kwalitatief) krijgt dan nu binnen het Targeting Center Borders beschikbaar is.
- Modus Operandi van illegale immigratie: de effectiviteit van indicatoren is afhankelijk van de kennis van modus operandi van mensen/organisaties die zich schuldig maken aan mensensmokkel- en mensenhandel. Ook hier geldt een voortdurende dynamiek.
- De mate waarin API-data zeggingskracht hebben over de intenties van passagiers is begrensd. Tijdens de interviews met DCG-medewerkers is dit naar voren gebracht en de beperking komt ook naar voren in de casuïstiek die we in dit rapport wordt beschreven. Op basis van API-gegevens kan voor sommige passagiers wel een vermoeden ontstaan dat er een risico is op irreguliere immigratie, echte harde aanwijzingen zijn het echter nooit. De meeste alerts zullen daardoor altijd blijven voortkomen directe matching met de databases en watchlist.

Afhandeling door grensdoorlaatposten

Met betrekking tot de praktijk van de verwerking van API-alerts bij de grensdoorlaatposten heeft dit onderzoek zich geconcentreerd op de praktijk op Luchthaven Schiphol. Hiervoor is gekozen omdat ruim 95% van de passagiersstromen van buiten Schengen (waarbij API een rol speelt) via deze luchthaven verloopt. Hier zijn in totaal acht doorlaatposten waarvan vijf posten aankomende passagiers verwerken. Eén van deze posten is een post die aankomende transferpassagiers verwerkt. Iedere doorlaatpost bestaat uit meerdere balies, aan het hoofd staat een groepscommandant. In principe komen alle API-alerts via een email terecht bij deze groepscommandanten. Met hen is afgesproken dat op alle alerts wordt geacteerd.

De groepscommandant zorgt ervoor dat de alerts worden uitgeprint en bij de balies komen te liggen. Ook is afgesproken dat over elke alert wordt teruggekoppeld aan het API-Centrum. In de terugkoppeling wordt

gemeld of de betreffende passagier is aangetroffen en het resultaat is geweest van de interventie. In 2016 is in 45% van de alerts geen terugkoppeling ontvangen, in 2017 is dat 60% en in het eerste kwartaal van 2018 40%. Dat er van veel alerts geen terugkoppeling is heeft voor een belangrijk deel te maken met het feit dat veel passagiers die op Schiphol aankomen doorvliegen naar een volgende bestemming en dus niet een Nederlandse grensdoorlaatpost passeren. Dit gaat om circa 37% van de passagiers. Alerts met een hoge prioriteit worden wel altijd opgevolgd, bijvoorbeeld via de inzet van DGC.

Casus 2: passagier met openstaande boetes
In de API-gegevens van een vlucht uit de Verenigde Staten naar Amsterdam vindt het API-Centrum een match met OPS. Het gaat om een reiziger met de Nederlandse nationaliteit. De reiziger heeft uiteenlopende boetes openstaan, waaronder veel verkeersboetes. Het gaat om ruim € 3.000.
Het API-Centrum verstuurt een alert met een lage prioriteit. De passagier kan door een grenswachter worden aangesproken op de boete, betaling kan echter niet worden afgedwongen (er was geen grond voor 'gijzeling').

Gemiddeld liggen er bij een balie van een grensdoorlaatpost zo'n vijf alerts. Het is belangrijk om het aantal beheersbaar te houden. Hierover wordt door een respondent opgemerkt:

> *'Je moet voorkomen dat er een hele stapel komt te liggen, want dan is het niet meer te overzien. Voortdurend worden er ook weer alerts tussenuit gehaald als we verwachten dat we de passagier niet meer zullen aantreffen.'*

Het werken met schriftelijke alerts werkt volgens de Brigade Grensbewaking goed. De grenswachten zijn erop getraind de alerts in zich op te nemen en in het achterhoofd te houden bij het controleren van passerende passagiers. Wel wordt daar meteen bij opgemerkt dat het wordt gezien als een tijdelijke oplossing. Uiteindelijk is het nadrukkelijk de wens om te komen tot een digitale oplossing. Hiermee zouden alerts niet langer op papier hoeven worden doorgegeven maar worden alle passagiers geautomatiseerd gescand. Van elke passagier wordt dan het reisdocument gescand en de gegevens vergeleken met o.a. de API-alerts. Zo'n systeem staat op de planning voor het eerste kwartaal van 2019 volgens de KMar. Bijkomend voordeel van zo'n systeem is dat van iedere alert ook een terugkoppeling wordt geregistreerd.

Bij elk gescand reisdocument krijgt de grenswacht dan meteen in beeld welke actie wordt voorgesteld door het API-Centrum als er een alert is uitgegaan, bijvoorbeeld welke aanvullende informatie nodig is om een verondersteld risico te verifiëren. Het scannen en de digitale verwerking kan per passagier mogelijk meer tijd in beslag nemen dan de manier waarop op dit moment passagiers worden gecontroleerd. Door meerdere

mensen binnen de KMar is aangegeven dat met de introductie van een digitale oplossing de capaciteit moet worden uitgebreid.

Afhandeling door Dedicated Gate Control (DGC)

De KMar beschikt op Schiphol over mobiele teams die aan de gate controles kunnen uitvoeren. Daar waar medewerkers van de grensdoorlaatposten op basis van een alert alleen gericht kunnen uitkijken naar iemand, kunnen medewerkers van DGC proactief een passagier aan de gate opwachten. DGC bestaat uit vier teams met elk ongeveer 6 mensen. Binnen de KMar is als uitgangspunt bepaald dat DGC altijd acteert op een alert met hoge prioriteit. Het API-Centrum geeft aan dat een alert met een hoge prioriteit moet worden geïnterpreteerd als een opdracht:

'Het is geen advies of een inzetverzoek'.

Men kan bij DGC wel bepalen welke opdracht wel en niet wordt uitgevoerd in de gevallen dat de capaciteit niet voorhanden is om alle alerts op te volgen. Regelmatig wordt DGC gedwongen keuzes te maken en bepaalt DGC voor iedere alert 'of zij er op gaan lopen of niet'. In hun overweging en beoordeling van API-alerts spelen vooral twee zaken:

1. de aard en ernst van de melding en
2. de bemensing/beschikbare capaciteit.

ad 1.) De aard en ernst van een melding:

Het API-Centrum geeft aan een alert een prioritering mee. De medewerkers van DGC maken ook een prioritering. De zaken die bij hen hoge prioriteit krijgen zijn vooral zaken die verband houden met een directe match vanwege een ernstig misdrijf en zaken, mede op basis van profielen en handmatige beoordeling, waarbij de kans groot is dat zij een potentieel slachtoffer kunnen onderscheppen. Naast DGC zijn er ook de reguliere grensdoorlaatposten die opvolging geven aan alerts.

Casus 3: vermoeden van mensensmokkel
Het API-Centrum vindt in de API-data een match met SISII. Aan boord van een vlucht uit een derde land zit een passagier die reist met een paspoort dat als vermist is opgegeven. Op basis van het PNR locator number dat in Nederland tot de API-set hoort, wordt vastgesteld dat de passagier samen reist met twee andere passagiers.
API-Centrum vermoedt dat de persoon die reist op het vermiste paspoort in werkelijkheid een kind is. Er is mogelijk sprake van mensensmokkel. Het API-Centrum verstuurt een alert met hoge prioriteit. Het gezelschap wordt bij aankomst door DGC aan de gate opgewacht. Het blijkt inderdaad om een kind te gaan, deze had echter wel een geldig paspoort maar het nummer daarvan bleek niet goed verwerkt en overeenkomstig met het nummer van het vermiste paspoort.

Ad 2.) Capaciteit en bemensing

Of op een API-alert door DGC wordt gereageerd, hangt tevens af van de bemensing. Ondanks het gegeven dat DGC op Schiphol met vier teams in principe altijd bemenst is, is zij niet altijd op volledige sterkte. Zo is de bezetting van DGC de afgelopen jaren teruggebracht, terwijl over dezelfde periode het aantal passagiers op de luchthaven substantieel is toegenomen. Bij het terugbrengen van de DGC capaciteit hebben budgettaire overwegingen een grote rol gespeeld.

Dat DGC niet op elke alert kan reageren, komt ook omdat dat tijdsintensief is. Wanneer op basis van een alert een gatecontrole wordt uitgevoerd, moeten soms alle passagiers van de vlucht worden gecontroleerd. Voor een intercontinentale vlucht kan het aantal te controleren passagiers oplopen tot 500. Het gemiddelde aantal passagiers per vlucht waarvoor de API-verplichten gelden is ruim 200. In de praktijk geldt dat voor vluchten uit sommige landen identiteitsverificatie lastig kan zijn vanwege de kwaliteit van pasfoto's of zelfs de beschikbaarheid van pasfoto's. Die foto's vormen overigens geen onderdeel van de API-data maar komen voort uit aanvullende bronnen die ter beschikking staan. Om de vertraging voor de passagiers zoveel mogelijk te voorkomen zet DGC daarvoor al snel zes mensen in.

Casus 4: passagier die nog een gevangenisstraf moet uitzitten

De API-gegevens van een persoon met de Nederlandse nationaliteit die reist van een derde land naar Amsterdam, matchen met OPS. De persoon blijkt voortvluchtig en moet nog een gevangenisstraf uitzitten van 183 dagen. Uit de bejegeningsgegevens van SISII blijkt dat de persoon mogelijk vuurwapengevaarlijk is. Deze melding – met hoge prioriteit – leidde tot een gatecontrole door DGC. De persoon is daarbij aangetroffen en aangehouden.

DGC heeft erop aangedrongen directer betrokken te zijn bij de screening van de API-data. Dit heeft ertoe geleid dat DGC zelf ook de beschikking heeft over de (geanonimiseerde) API-bestanden. Naast de dataverwerking door het API-Centrum, monitoren de medewerkers van DGC zelf ook de risico's op illegale immigratie aan de hand van (geanonimiseerde) API-bestanden. DGC leidt risico's af door te na te gaan of er afwijkingen zijn op de normaalsituatie. Hiervoor ontvangen zij van het API-Centrum de geanonimiseerde databestanden van binnenkomende vluchten (van buiten het Schengengebied). Deze databestanden bevatten uitsluitend gegevens uit de API-set, exclusief de namen van passagiers.

Gebruik door Bureau Asielzaken KMar

Naast de grensdoorlaatposten en DGC ontvangt het Bureau Asielzaken van de KMar ook API-alerts. Het Bureau Asielzaken handelt alle asielaanvragen af. Dat zijn er gemiddeld ongeveer vijf per dag. Het Bureau Asielzaken komt echter zelf nooit in actie naar aanleiding van

een alert. Wel maakt het bureau gebruik van het API-Centrum. Zij vraagt standaard voor elke persoon die asiel aanvraagt, de API-gegevens op. Aan de hand hiervan kunnen zij van een passagier die zich correct identificeert en in sommige gevallen ook wanneer een passagier zich niet helemaal correct identificeert snel en betrouwbaar verifiëren met welke luchtvaartmaatschappij en via welke route hij/zij naar Nederland is gekomen. Het is informatie die belangrijk kan zijn voor de reconstructie van het vluchtverhaal door de IND. Het is ook informatie die gebruikt kan worden om een terugvlucht bij een luchtvaartmaatschappij te claimen om het moment dat de asielaanvraag wordt afgewezen.

Aanlevering gegevens via Pi-NL

Naast de aanlevering van API-gegevens rechtstreeks aan KMar is er ook nog een tweede gegevensstroom met een bredere set gegevens die de luchtvaartmaatschappijen verplicht moeten aanleveren bij vluchten van en naar Nederland. Die bredere stroom bestaat uit de beschikbare PNR-gegevens bij PI-NL. Deze tweede stroom gaat nu alleen naar de Douane.

Er is op dit moment geen relatie tussen de twee systemen. De voor de KMar TCB/API-Centrum vanuit de richtlijn 2004/82 EG verzamelde API-gegevens worden rechtstreeks aan de KMar gestuurd. Op grond van de PNR-richtlijn worden deze gegevens na het in werking treden van de PNR-wet *ook* aangeleverd bij Pi-NL. Zoals gezegd: de Douane krijgt die gegevens nu al via TRIP. Pi-NL gaat gebruikmaken van de Travel Information Portal (TRIP) applicatie voor de ontvangst en verwerking van PNR- en API-gegevens binnen de doelbinding van de PNR Richtlijn 2016/681. Opsporingsdiensten kunnen op grond van een verordening via TRIP gericht reisgegevens opvragen bij Pi-NL ten behoeve van een strafrechtelijk onderzoek naar terrorisme of andere criminaliteit.

De TRIP-applicatie die sinds 2016 door de Douane in gebruik is[32] bestaat uit twee delen. Het eerste deel (TRIP Single Window) is erop gericht alle passagiersgegevens (PNR inclusief API) te ontvangen. Het tweede deel (TRIP Applicatie) wordt gebruikt om de ontvangen gegevens te analyseren, te vergelijken met de door de minister aangewezen opsporingsregisters en profielen en voor het verwerken van informatie verzoeken.

In het gebruik van API-data voor de API-richtlijn en de PNR-data voor Pi-NL vanuit de PNR-richtlijn zitten verschillen vanwege de doelbindingen van beide richtlijnen. De doelbinding bij de API-richtlijn is het verbeteren van grenscontroles en het bestrijden van illegale migratie. De doelbinding bij PNR-richtlijn en daarmee ook de PNR-data (inclusief de API-data) die aan Pi-NL wordt aangeleverd is het bestrijden van ernstige criminaliteit en terroristische misdrijven. Er wordt op dit moment verkend of TRIP Single Window ook te gebruiken is voor de KMar omdat het om dezelfde API-gegevens gaat.

[32] https://www.rijksoverheid.nl/onderwerpen/luchtvaart/reisgegevens-luchtvaart

4 Evaluatie van meerwaarde en verbetermogelijkheden

4.1 Meerwaarde van API

De in het tweede hoofdstuk beschreven veronderstellingen die aan de introductie van de API-verplichting ten grondslag liggen, worden door alle respondenten binnen de KMar onderschreven. Zij ervaren de grenscontrole erdoor wordt verbeterd en dat het gebruik van API-gegevens bijdraagt aan de doorstroom van passagiers aan de grensdoorlaatposten. De bevindingen op dit onderdeel sluiten aan bij eerdere evaluaties en duiden daarmee op een duidelijk effect van het gebruik van API en structurele meerwaarde. In deze paragraaf beschrijven we de meerwaarde in kwalitatieve zin op basis van ervaringen van medewerkers van het API-Centrum, DGC en de grensdoorlaatposten.

Verbeteren van grenscontrole: meer tijd om de passagier te controleren
Het API-Centrum heeft betere en gerichtere mogelijkheden dan een grenswacht aan een doorlaatpost om passagiers te matchen aan een watchlist, opsporingsdatabase of profiel. Het API-Centrum kan bijvoorbeeld ook matchen op basis van gelijkende namen, zoals beschreven in paragraaf 3.3 (onder a. Directe matching). Bij het API-Centrum heeft men de gelegenheid om passagiers nader te beoordelen die gelijkende namen hebben met personen die gesignaleerd staan vanwege terrorisme. Vanaf het moment van het verzenden van de API-batch tot vlak voor landing van het vliegtuig is er bij het API-Centrum de tijd om de mogelijkheden van de vergelijkingen te benutten. Bij signaleringen met hoog veiligheidsrisico is daardoor langer de gelegenheid om met meerdere matchingsvarianten (en daarmee meer uitkomsten/false positives) toch de juiste persoon te kunnen onderkennen. Er is daarbij ook gelegenheid tot onderling overleg (het vierogenprincipe). De grenswacht aan de grensdoorlaatpost heeft deze mogelijkheden niet.

Verbeteren van grenscontrole: verder kunnen kijken dan een register
Een voordeel van API-gegevens is dat niet alleen passagiers worden gesignaleerd die zijn opgenomen in een opsporingsregister of watchlist. API biedt de mogelijkheid op basis van profielen om breder te kijken en ook passagiers te onderkennen die niet in een opsporingsregister of watchlist staan maar waarbij uit de gegevens wel een aanleiding kan worden afgeleid om nader onderzoek te doen. Aan een grensdoorlaatpost is zo'n analyse niet uit te voeren als passagiers één voor één zich melden. De 'unknown passengers with unknown risk' komen zonder API niet in beeld.

Een medewerker van het API-Centrum merkt in dit kader op - verwijzend naar casus 5 - :

'Er zijn bijzonderheden die een grenswacht aan een doorlaatpost niet kan onderkennen. Er is op het eerste gezicht niets verdachts aan een jonge vrouw uit een derde land. Dat zo iemand mogelijk onder invloed staat van een bende mensenhandelaars zie je pas als je ziet dat zij samen reist met iemand die eerder is veroordeeld voor mensenhandel'.

Casus 5: voorkomen van mensenhandel

De KMar ontvangt van een buitenlandse partner het bericht dat een bende van smokkelaars in een derde land onder valse voorwendselen meisjes ronselt voor prostitutie in een EU-lidstaat. De meisjes wordt voorgehouden daar als au pair te kunnen gaan werken. Er is inmiddels een patroon ontdekt. Het gaat om meisjes in een bepaalde leeftijdscategorie die steeds reizen vanaf een bepaalde luchthaven en via Amsterdam naar een stad in een EU-lidstaat vliegen.

Op basis van dit patroon wordt een profiel opgemaakt. Met dit profiel worden met behulp van een zoekmachine passagiers geselecteerd waarvan API-gegevens overeenkomsten hebben met de slachtoffers die eerder zijn gesignaleerd.

De gegevens van deze passagiers worden verwerkt door de medewerkers van het API-Centrum en worden als API-alert uitgezet bij de grensposten met daarbij de opdracht om aan betrokken passagiers enkele vragen te stellen over de verwachtingen van hun verblijf op de plaats van bestemming.

Hetzelfde geldt voor een passagier aan wie bij een grensdoorlaatpost op basis van een face-to-face-contact niets bijzonders opvalt, maar waarbij wel bijzonderheden zichtbaar worden wanneer de vluchtgegevens in de controle worden betrokken. Een voorbeeld hiervan is beschreven als casus 6.

Casus 6: onderkennen van een mogelijke asielzoeker
In de API-gegevens van een vlucht uit een derde land valt een passagier op vanwege zijn nationaliteit en de reisroute. De passagier reist volgens de API-gegevens via Schiphol door naar een volgende bestemming. De combinatie van nationaliteit en route wordt getypeerd als ongebruikelijk en kan een aanwijzing zijn dat het niet de bedoeling van de passagier is om over te stappen op Schiphol maar er asiel aan te vragen.

Om te voorkomen dat hij pas in beeld komt bij een Nederlandse grenspost en zich daar zonder reisdocument voordoet als een staatsburger komende uit een land waarvoor de kans groter is dat asiel wordt verleend, wordt een API-alert verzonden om de passagier aan de gate bij aankomst van het vliegtuig op te wachten om na te gaan wat zijn bestemming is. Bij de gate blijkt dat de passagier inderdaad asiel wil aanvragen. Deze wordt in behandeling genomen. Mocht de betrokkene in een later stadium worden teruggestuurd, dan is aan de hand van de API-gegevens de Brigade Vreemdelingenzaken van KMar in staat een terugvlucht te claimen bij de betrokken luchtvaartmaatschappij.

Verbeteren van grenscontrole: werken met matchingscriteria

Binnen de KMar en in internationaal verband wordt voortdurend kennis uitgewisseld over actuele ontwikkelingen, vluchtelingenstromen en ontwikkelingen met betrekking tot grensgerelateerde criminaliteit (zoals mensensmokkel en -handel). Het streven is om alle KMar-medewerkers op Schiphol voortdurend op de hoogte te houden van deze kennis om hen vervolgens te laten uitkijken naar de passagiers die mogelijk in verband staan met die ontwikkeling. Het is in de praktijk lastig om de medewerkers voortdurend opnieuw te instrueren over wat zij precies met deze kennis kunnen doen. Een respondent van de KMar zegt hierover:

> *'We kunnen niet alle 700 grenswachten voortdurend op de hoogte houden'.*

Met behulp van de API-gegevens kan de kennis over actuele ontwikkelingen worden omgezet naar concrete alerts. De effectiviteit van een grenswacht is daardoor minder afhankelijk van zijn kennis over actuele ontwikkelingen en zijn vermogen om dit toe te passen. Zijn effectiviteit is meer afhankelijk geworden van zijn alertheid en vermogen om mensen van wie zij een alert op hun desk hebben liggen, te herkennen. Met andere woorden: API stelt de KMar in staat om kennis over illegale immigratie en grensoverschrijdende criminaliteit te vertalen naar gerichtere controles van passagiers en gerichtere inzet

van capaciteit. Meerdere keren is in de gesprekken met KMar-medewerkers als voorbeeld verwezen naar de actualiteit rond een groep mensen die ergens in de wereld onder druk staan als gevolg van politieke of economische omstandigheden. De actualiteit kan ertoe leiden dat er onder deze groep weer meer mensen zullen zijn die vluchten (onder andere naar Nederland). Het API-Centrum kan daarop anticiperen en grenswachten gericht laten uitkijken.

Planning van personele capaciteit

Door het API-Centrum is verder aangegeven dat API bijdraagt aan een betere planning van de inzet van grenswachten en hun ondersteuning aan de grens. Op basis van API-gegevens kan worden voorspeld op welk moment waar op de luchthaven meer capaciteit nodig is om nader onderzoek te doen naar passagiers. Dit komt de effectiviteit van de grenscontrole ten goede en ook de efficiëntie. Een medewerker van het API-Centrum:

> *'Wanneer er op een bepaalde pier een of meerdere vluchten aankomen van luchthavens waar vaker asielzoekers vandaan reizen, en wanneer op die vluchten ook meerdere passagiers zitten die opvallen, dan weten we dat het op bepaalde doorlaatposten druk wordt. De bemensing kan dan worden aangepast'*.

Er kunnen meer posten worden bemand en eventueel kan ook de capaciteit van de backoffice worden uitgebreid: de unit die nader onderzoek uitvoert of bij de Brigade Vreemdelingenzaken die asielaanvragen afhandelt. Ook kunnen daar eventueel extra tolken beschikbaar worden gesteld die de taal van de betreffende passagiers beheersen.

> *'Die tolken kunnen dan tijdig worden ingezet. We hebben een tolkenbureau achter de hand. Die kunnen telefonisch assisteren'*.

In hoeverre API tot nu toe daadwerkelijk ondersteunt bij de personele planning, is met dit onderzoek niet nagegaan.

Doorstroom: grensdoorlaatposten worden ontlast

API data zijn van belang bij het naleven van de verplichting van systematische grenscontrole conform Schengengrenscode. Voor deze evaluatie hebben we niet onderzocht welke tijdsbesparing er per passagier is gerealiseerd dankzij het gebruik van API. Dat is alleen kwalitatief te beschrijven. Met de huidige passagiersaantallen op de Luchthaven Schiphol wordt het vrijwel onmogelijk geacht iedere binnenkomende passagier aan een grensdoorlaatpost te controleren op de aspecten die in de Schengengrenscode worden benoemd (identiteit, geldigheid reisdocument, signalering in OPS, SISII, gevaar openbare orde, nationale veiligheid, etc.), zonder dat dat leidt tot ernstig oponthoud. De controle op al deze aspecten neemt bij een grensdoorlaatpost al snel 15 seconden per passagier in beslag. Bij een gezin met drie kinderen gaat het al snel om meer dan een minuut. Bij de huidige omvang van het grensverkeer op de luchthaven – van tienduizenden passagiers per dag – gaat het om veel tijd en capaciteit. Door de matching met OPS, SISII en de watchlist met behulp van de API-gegevens vooraf te laten doen door het API-Centrum kunnen de

handelingen aan de grensdoorlaatpost bij het leeuwendeel van de passagiers zich beperken tot verificatie van de identiteit en de echtheid en geldigheid van reisdocumenten.

De verbeterde doorstroom is niet alleen voor de KMar van meerwaarde. Voor de passagiers voorkomt het lange wachttijden. De luchtvaart-maatschappijen, ook in IATA-verband, zien een snellere doorstroming als een bijdrage aan de kwaliteit van de reiservaring (IATA, 2017).

Claimen van passagiers bij luchtvaartmaatschappijen

API-gegevens helpen bij het claimen van passagiers bij luchtvaartmaatschappijen in het kader van de Carrier Liability. Luchtvaartmaatschappijen die passagiers hebben vervoerd zonder geldig reisdocument of van wie anderszins op voorhand duidelijk was dat hen de toegang zou worden geweigerd, zijn verplicht de betreffende passagiers weer mee terug te nemen, eventueel op een later moment. Aan de hand van API kan de KMar van een passagier makkelijker vaststellen met welke luchtvaartmaatschappij de passagier is gekomen, en naar welke bestemming hij moet worden uitgezet. Binnen de Brigade Vreemdelingenzaken van de KMar is met name het team 'Claims en Art. 4 (CIA)' bezig met het claimen van passagiers. Mede dankzij API kunnen zij van circa 95% van de uit te zetten passagiers vaststellen met welke luchtvaartmaatschappij zij gekomen zijn. Bij de overige 5% is dat niet mogelijk bijvoorbeeld omdat de passagier een ander reisdocument gebruikt om Nederland binnen te komen en het document dat is gebruikt voor de API-data niet meer kan overhandigen. Het scheelt aanzienlijk in de kosten wanneer niet de KMar maar de luchtvaartmaatschappij de kosten voor haar rekening neemt.

Gebruik API-data voor opsporing en onderzoek

API-data kunnen in geanonimiseerde vorm worden gebruikt bij opsporingsonderzoeken en onderzoeksdoeleinden binnen de doelbinding van de Vreemdelingenwet. Het kan hierbij gaan om ontwikkelingen in de samenstelling van passagiersstromen te bepalen vanaf bepaalde locaties. Deze informatie kan bijvoorbeeld worden gebruikt om profielen te ontwikkelen voor de detectie van 'unknown persons, with unknown risk'. De gegevens zijn nodig om te bepalen wat een normaal beeld is op een bepaalde vlucht en om te beoordelen welke veranderingen in dit beeld optreden.

Veiligheid aan boord

De luchtvaartmaatschappijen en IATA geven aan dat de API-verplichting, zeker na de volgende stap in het kader van Smart Borders, bijdraagt aan de veiligheid aan boord. Passagiers worden dan bij het boarden gecontroleerd. Het gaat hierbij nadrukkelijk niet om een grenscontrole maar om de controle of een passagier toestemming krijgt te reizen. De medewerkers aan de gate krijgen direct via een interactieve verbinding met de autoriteiten in het bestemmingsland te horen of de betreffende passagiers aan boord mogen of niet. Het voorkomt dat mensen aan boord komen die maatschappijen liever niet aan boord hebben omdat de betreffende passagiers ook andere

passagiers in gevaar kunnen brengen. Met het toekomstige Smart Border systeem wordt bovendien zoveel mogelijk voorkomen dat de maatschappijen voor eigen rekening mensen terug moeten vervoeren die niet worden toegelaten.

4.2 Aandachtspunten

In de interviews met de verschillende KMar medewerkers zijn ook punten genoemd die voor verbetering vatbaar zijn.

Behoefte aan adequate voorziening om alerts aan de grens te krijgen

Op dit moment worden de API-alerts door het API-Centrum per e-mail gestuurd naar de groepscommandanten van de grensdoorlaatposten. Deze printen de alerts uit en zorgen ervoor dat ze komen te liggen op de desks van de grenswachten. Deze manier van werken doet een groot beroep op de oplettendheid van de grenswachten. Iedere grenswacht heeft op zijn desk gemiddeld vijf API-alerts liggen. Van de grenswacht wordt verwacht die alerts in zich op te nemen en de betreffende passagiers ook daadwerkelijk te herkennen op het moment dat zij de grens willen passeren. Volgens de geïnterviewde KMar-medewerkers zijn de grenswachten voldoende alert. Het is echter niet vast te stellen of dat daadwerkelijk zo is en of en hoe vaak het voorkomt dat een gesignaleerde passagier er tussendoor glipt. Het is op voorhand duidelijk dat niet alle gesignaleerde passagiers ook aan de grens kunnen worden opgemerkt, omdat alerts betrekking hebben op passagiers die doorreizen naar een andere bestemming en derhalve op Schiphol geen grenspost passeren. Afgezien van de vraag hoeveel passagiers worden gemist, is het de betrokken KMar-medewerkers duidelijk dat de huidige werkwijze (van het schriftelijk doorgeven van alerts) niet meer van deze tijd is. Betrokkenen bij DGC zien uit naar een elektronisch systeem, waarbij gesignaleerde personen automatisch worden gedetecteerd en niet langer alleen op basis van observatie van grenswachten. De KMar verwacht dat zo'n systeem in het eerste kwartaal van 2019 in gebruik wordt genomen.

Systematische detectie van unknown persons with an unknown risk

API-gegevens bieden meer mogelijkheden om passagiers die niet staan gesignaleerd in een opsporingssysteem maar toch nadere aandacht behoeven, te detecteren. Het betreft met name de detectie van 'unknown persons with an unknown risk', die op basis van de combinatie persoons- en reisgegevens uit de passagiersstroom gefilterd kunnen worden. Hiervoor kunnen algoritmes worden gebruikt waarmee systematisch gezocht kan worden naar afwijkende patronen. De ontwikkelingen van deze algoritmes en de voortdurende toetsing en aanpassing is nog niet systematisch opgepakt. Capaciteitsgebrek speelt hierbij een rol. De detectie van deze categorie van passagiers binnen het API-Centrum en bij DGC vindt nu nog handmatig plaats. Dit heeft twee inhoudelijke nadelen. In de eerste plaats is de detectie afhankelijk van de oplettendheid, kennis en ervaring van een individuele medewerker, in de tweede plaats wordt hierdoor niet systematisch gescreend: niet alle passagiers worden op een afwijkende of opvallende

combinaties van kenmerken gescreend. Binnen het API-Centrum bestaat de wens om meer systematiek te brengen in de handmatige controle zodat steeds duidelijk is op basis van welke combinaties en criteria wordt gealerteerd. Het biedt ook de mogelijkheid om in internationaal verband af te stemmen over hoe actuele risico's het best gedetecteerd kunnen worden.

Bezetting API-Centrum

De uren waarop dagelijks de vluchten van buiten het Schengengebied binnenkomen, komen niet overeen met de uren waarop het API-Centrum bemand is. Met name in de vroege ochtend is er altijd een periode waarop er geen API-alerts worden gegenereerd. Dit betekent overigens niet dat er helemaal geen alerts zijn voor vluchten die dan binnenkomen. Veel vluchten zijn immers intercontinentaal en zijn vaak al de dag ervoor verwerkt.

Volledigheid vluchtgegevens

Binnen de API-gegevensset is het vertrekpunt en het aankomstpunt van het vliegtuig een verplicht in te vullen veld. Voor passagiers met een overstap betekent dit dat soms niet bekend is waar zij hun reis zijn begonnen en/of wat hun eindbestemming is. Veel luchtvaartmaatschappijen leveren deze gegevens wel zonder dat zij daartoe verplicht zijn. Er zijn volgens de KMar echter ook buitenlandse maatschappijen die dat niet doen. Het kunnen beschikken over deze gegevens zorgt voor betere analysemogelijkheden.

Opvolging van alerts

Kijkend naar de praktijk waarin API-gegevens worden verwerkt en gebruikt blijkt dat er een waterscheiding zit tussen signaleren en acteren. Signaleren gebeurt op het API-Centrum, acteren gebeurt bij de grensdoorlaatposten en door DGC. In de praktijk blijkt dat de eenvoud waarmee een alert wordt gegeven niet in verhouding staat tot de moeite die het kost om er vervolgens op te acteren, met name door DGC. Zoals beschreven, houdt een actie soms in dat meerdere medewerkers veel passagiers van een vlucht moeten controleren. Het leidt ertoe dat op een deel van de alerts niet wordt gereageerd door DGC. Hoe vaak en in welke mate dit voorkomt is niet duidelijk. Veel hangt af van het beoordelingsvermogen van de KMar medewerkers die op een zeker moment DGC bemensen en het aantal mensen dat daar verder paraat is. Alerts met een hoge prioriteit worden in beginsel altijd opgevolgd ook als het gaat om transfer passagiers. Het komt echter voor dat er keuzes gemaakt moeten worden. Het risico is daarmee groot dat DGC vooral op alerts loopt gebaseerd op een match met OPS en/of SISII, in het kader van strafrechtelijke opsporing en minder in het kader van illegale immigratie. Dit risico is genoemd in de interviews en tijdens de twee ochtenden waarop we hebben meegelopen op de werkvloer.

Registratie terugkoppeling alerts

Niet van alle alerts is een terugkoppeling verwerkt in de registraties. In het eerste kwartaal van 2018 is van 40% van alle alerts geen terugkoppeling ontvangen. Over heel 2017 is dat bij 60% van de alerts het geval. Een aantal redenen hiervoor kan de KMar benoemen:

- Een groot deel van de passagiers die op Schiphol aankomen reizen direct verder en komen niet langs de grensdoorlaatposten. Het gaat hier om in 2017 om 37% van de reizigers.
- Boetes worden geïnd via een betaalzuil en niet in een systeem gemuteerd, als de alert niet wordt teruggekoppeld, wordt deze niet gevonden in een van de systemen dus teruggekoppeld als 'geen terugkoppeling ontvangen'.
- Het was een lange tijd niet mogelijk om een KMar medewerker op de alert toe te voegen, hierdoor was het niet mogelijk iemand aansprakelijk te maken voor een terugkoppeling.
- In 2018 is het weer mogelijk om dagelijks een export te sturen met openstaande alerts naar de chef van dienst.
- Er zijn wisselingen geweest met aanspreekpunten op de grensbewaking. Het niet voldoende naleven van afspraken rond het invoeren van de terugkoppelingen is daar een gevolg van.

Bij een groot deel van de alerts is daarmee onduidelijk wat er uiteindelijk mee is gedaan. Deze terugkoppelingen zijn naar onze mening van belang om de effectiviteit van de alerts te monitoren. Met die terugkoppeling is het mogelijk de analyses en profielen te verbeteren en door te ontwikkelen. Volgens het TCB wordt in het eerste kwartaal van 2019 een systeem in gebruik genomen waarbij van alle passagiers die een grensdoorlaatpost passeren een geautomatiseerde vergelijking met de actuele alerts wordt gemaakt. De terugkoppelingen op de alerts worden op die manier volledig.

5 Conclusies

Sinds 2009 maakt de KMar bij de uitvoering van haar grenscontroletaken gebruik van API-gegevens. Wat begon met enkele vluchten van de KLM, is inmiddels een verplichting geworden die geldt voor elke luchtvaartmaatschappij die van buiten Schengen en EU naar een Nederlandse luchthaven vliegt. Nederland implementeert hiermee een Europese richtlijn waaraan ook alle andere EU-lidstaten gebonden zijn. De richtlijn sluit aan op het mondiaal initiatief van de Internationale Burgerluchtvaart Organisatie van de Verenigde Naties (ICAO) om passagiersgegevens te gebruiken bij het grensbeheer. Nederland heeft de Europese API-richtlijn geïmplementeerd in de Vreemdelingenwet. Met dit onderzoek is nagegaan hoe uitvoering wordt gegeven aan de verplichting en wat dat oplevert voor het grensbeheer. De onderzoeksvragen die in paragraaf 1.4 zijn opgenomen zijn niet kort stuk voor stuk te beantwoorden. Veel vragen hangen met elkaar samen en de antwoorden vragen toelichting en nuancering. De antwoorden hebben we in dit hoofdstuk zoveel mogelijk gegroepeerd.

Ervaringen van luchtvaartmaatschappijen

De ervaringen van de luchtvaartmaatschappijen komen aan de orde in onderzoeksvraag 1 en 2. Hoewel de API-verplichting bij luchtvaartmaatschappijen investeringen vergt en voortdurende aandacht vraagt van grondpersoneel, cabinepersoneel en medewerkers van de backoffice (waaronder security, business regulation en systeembeheer), zijn de benodigde handelingen onderdeel geworden van de dagelijkse routine. Dat geldt althans voor de drie Nederlandse luchtvaartmaatschappijen die wij in het kader van dit onderzoek spraken. Handelingen die nodig zijn vanwege de API-verplichting zijn daar in hoge mate ingebed in het proces dat loopt van de (online) ticketverkoop tot aan het moment dat een vliegtuig opstijgt. Wat de belasting die uitgaat van de API-verplichting, verder enigszins relativeert, is dat de belangrijkste bestemmingen (landen) waarop gevlogen wordt API-verplichtingen opleggen. Vrijwel *alle* andere luchtvaartmaatschappijen hebben er daardoor ook mee te maken. Het is daarmee geen verstoring van de concurrentiepositie van de maatschappijen. De API-verplichting is in de ogen van de luchtvaartmaatschappijen er één die er inmiddels bij hoort, net als alle andere voorschriften en procedures die kenmerkend zijn voor de luchtvaartsector.

De naleving van de API-verplichting is hoog. Bij zowel de drie luchtvaartmaatschappijen die wij in het kader van dit onderzoek spraken als bij de KMar zijn geen boetes bekend. De KMar spreekt van 100% compliance: voor alle API-plichtige vluchten worden de API-gegevens van alle passagiers aangeleverd door alle maatschappijen. Voor zover zij weten is er in Nederland nog nooit een sanctie opgelegd vanwege overtreding van de API-regels. Het komt overigens incidenteel wel voor dat voor een vlucht de gegevens *niet* zijn geleverd. Dit wordt volgens betrokkenen altijd in goed overleg opgepakt. De

luchtvaartmaatschappijen zijn zeer te spreken over de samenwerking met de KMar.

Ontwikkeling gebruik van API-gegevens

Het aantal passagiers dat van buiten het Schengengebied naar Nederland reist, is in het afgelopen decennium vrijwel ieder jaar gestegen. Het aantal passagiers waarvoor API-gegevens is ontvangen is sinds 2013 sterk gegroeid van 200.000 tot ruim 1 miljoen per maand. Daarbij speelt vooral een grote rol dat in deze periode het aantal luchthavens waarvoor de verplichting geldt API-gegevens te leveren is toegenomen. Vanaf 1 juni 2016 is de verplichting van kracht voor alle luchthavens van buiten het Schengengebied en alle passagiers. Daarnaast is ook het aantal API-velden uitgebreid. Deze uitbreiding sluit aan bij toezeggingen die de staatsecretaris heeft gedaan in aansluiting op het vorige evaluatieonderzoek (brief van de staatssecretaris, 25 juli 2014). Het effect van de uitbreiding van het aantal luchthavens is goed te zien in de ontwikkeling van het aantal vluchten vanaf 2013. Het aantal voor API relevante inkomende vluchten neemt toe van 3.000 eind 2013 tot gemiddeld 5.000 per maand in 2017 en de eerste 3 maanden van 2018.

De ontwikkeling van het aantal matches in de periode 2013-september 2016 verloopt grillig. In de maanden na oktober 2016 tot en met de laatste gegevens van maart 2018 is een stabilisering te zien. Een verklaring voor deze ontwikkeling is gelegen in de verbeteringen die in de afgelopen jaren zijn gerealiseerd in de verschillende opsporingsregisters en watchlists en de ervaring die is opgedaan met het werken aan en met profielen om passagiers met een verhoogd risico op illegale immigratie te detecteren. In de periode vanaf januari 2017 tot en met maart 2018 schommelt het aantal matches tussen de 4.500 en 8.000.

Niet elke match leidt tot een alert voor de grensdoorlaatposten of aan DGC. In het screeningsproces wordt rekening gehouden met bijvoorbeeld typefouten, spellingsvarianten, verschillende manieren van noteren. Tussen match en alert zitten medewerkers van het API-Centrum die op basis van bronnen, hun ervaringen en onderlinge kennisuitwisseling, inschatten welke signalen en welke passagiers werkelijk aandacht behoeven. Het aantal API-alerts is in de afgelopen jaren gestaag toegenomen van zo'n 200 per maand in 2013 naar circa 1.200 per maand in 2018. Hierbij moet worden opgemerkt dat de gegevens over deze langere periode niet goed zijn te vergelijken. In 2013 gold de verplichting voor 54 luchthavens en dit aantal is in enkele stappen uitgebreid. Pas na juni 2016 worden de API-gegevens van alle luchthavens buiten Schengen verwerkt. Bovendien is volgens de ervaringen van KMar de kwaliteit en actualiteit van de verschillende opsporingsdatabases steeds beter. Het aantal alerts volgt de groei van het grensverkeer en blijft stabiel op circa 0,1% van het aantal passagiers.

In 2016 en 2017 is aantoonbaar op basis van de geregistreerde terugkoppelingen aan circa 120 mensen formeel de toegang geweigerd. In het eerste kwartaal van 2018 gaat het om 46 mensen.

Met behulp van de API-gegevens kan volgens opgave van de KMar 95% van de passagiers waarvan de toegang wordt geweigerd bij de luchtvaartmaatschappijen worden geclaimd. Dankzij API is vast te stellen met welke vlucht en luchtvaartmaatschappij iemand is aangekomen in Nederland.

Verhouding API en TRIP

Onderzoeksvraag 5 gaat over de relatie API en TRIP. De KMar TCB/API-Centrum krijgt de API-gegevens via een broker van de verschillende luchtvaartmaatschappijen. Daarbij wordt op dit moment geen gebruikgemaakt van TRIP. Het API-Centrum is opgezet voordat TRIP bestond. Er wordt wel verkend of ook de KMar TCB/API-Centrum gebruik kan gaan maken van TRIP Single Window. Luchtvaartmaatschappijen hoeven de passagiersgegevens die zij verplicht zijn te verstrekken dan maar bij één loket aan te leveren.

De Douane gebruikt TRIP al sinds 2016 voor de ontvangst, verwerking en analyse van passagiersdata. Indien de PNR-wet wordt aangenomen krijgt Pi-NL in een aparte gegevensstroom op grond van een aparte richtlijn en wetsvoorstel ook passagiersgegevens. Pi-NL gaat gebruikmaken van TRIP voor de ontvangst en verwerking van de beschikbare PNR-gegevens (inclusief de API-gegevens). De verwerking valt binnen de doelbinding van de PNR Richtlijn 2016/681.

TRIP wordt straks in Pi-NL gebruikt om alle dataproducten (PNR-gegevens inclusief API-gegevens) namens de Nederlandse overheid te ontvangen. In TRIP worden deze gegevens geanalyseerd en vergeleken met de door de minister aangewezen databases (zoals SISII en OPS), watchlists en profielen en voor het verwerken van informatie verzoeken. Daarnaast wordt TRIP ook gebruikt voor het verwerken van informatieverzoeken.

De (concept)-wet op het gebruik van passagiersgegevens ten behoeve van bestrijding ernstige criminaliteit en terrorisme voorziet in de bevoegdheid om naast PNR-gegevens ook de door de lidstaat gevraagde API-data te gebruiken. Dat betekent voor de Nederlandse situatie dat in ieder geval voor alle vluchten komende van buiten de EU naar een Nederlandse luchthaven de betreffende API-dataset samen met de PNR-gegevens verstrekt worden aan Pi-NL. In het gebruik zitten verschillen vanwege de doelbindingen van beide richtlijnen. De doelbinding bij de API-richtlijn is het verbeteren van grenscontroles en effectief illegale immigratie bestrijden. De doelbinding bij PNR-richtlijn is het bestrijden van ernstige criminaliteit en terroristische misdrijven.

Meerwaarde van API-gegevens voor grenscontrole

API-gegevens worden verondersteld de grenscontrole zodanig te ondersteunen dat het zowel de effectiviteit als de efficiëntie van de grenscontrole verbetert. Dit is de essentie van onderzoeksvraag 8. Deze

meerwaarde wordt in de gesprekken met de KMar bevestigd. In de kern komt het erop neer dat grensautoriteiten hun controle van een passagier al kunnen uitvoeren voordat deze zich aan de doorlaatpost bekend maakt. Dankzij API weten zij al eerder welke en hoeveel passagiers op een luchthaven aankomen en vervolgens mogelijk een grensdoorlaatpost passeren. De grensautoriteiten kunnen dankzij API analyses uitvoeren en anticiperen op mogelijke interventies op basis van de beschikbare informatie.

Het voorwerk houdt in dat van iedere passagier die van buiten Schengen naar Nederland reist wordt nagegaan of deze staat gesignaleerd in een database (OPS/SISII) of op een watchlist of dat nadere aandacht vereist is vanwege ongebruikelijke of opvallende combinaties van persoons- en vluchtkenmerken. Het gebruiken van profielen is niet mogelijk zonder API. Een grenswacht aan een grensdoorlaatpost kan niet zien of een passagier lid is van een reisgezelschap dat mogelijk extra aandacht nodig heeft. API maakt de grenscontrole daarmee effectiever.

Door dit proces door het API-Centrum te laten doen wordt aan de grensdoorlaatpost per passagier enkele seconden aan tijd bespaard. Binnen de KMar wordt breed aangegeven dat deze seconden met de huidige passagiersaantallen een substantiële bijdrage leveren aan de doorstroom bij de grensposten. Die doorstroming is niet alleen voor de reiziger prettig en daarmee ook voor de luchtvaartmaatschappijen gezien het belang dat zij hebben bij een positieve klantervaring rond luchtreizen. Zonder het gebruik van API-gegevens en de screening van het API-Centrum zouden veel meer capaciteit en mogelijk ook meer voorzieningen nodig zijn aan de grensdoorlaatposten om iedere passagier volgens de bepalingen van de Schengengrenscode te controleren. Bovendien kan de capaciteit nu gericht worden ingezet op de plekken en momenten waar die nodig is. Bijvoorbeeld omdat er een vlucht binnenkomt met veel passagiers met een alert of een passagier met een zeer hoge prioriteit. Daarmee dragen API-gegevens bij aan de efficiëntie van de grenscontroles.

Ook wordt onderkend dat de grenscontrole met API inhoudelijk is verbeterd. In de eerste plaats bieden API-gegevens de mogelijkheid om in een backoffice (het API-Centrum) meer tijd te besteden aan de matching van passagiers met opsporingssystemen. In het API-Centrum heeft men meer tijd om een match nader te onderzoeken en na te gaan welke andere passagiers eventueel gelieerd kunnen worden aan een match. Ook heeft men bij het API-Centrum meer tijd om passagiers te controleren die in eerste instantie niet matchen met een opsporingsregister of een watchlist maar waarvan de namen wel gelijkenis hebben met personen uit deze registers en watchlist. In de tweede plaats bieden API-gegevens de mogelijkheid om passagiers te detecteren die weliswaar niet staan gesignaleerd maar waarvan de combinatie van reis- en persoonsgegevens wel vraagt om een nader onderzoek (bevraging van de passagier). De casuïstiek en interviews leren dat hiermee niet alleen daders worden onderkend maar ook (potentiële) slachtoffers in beeld komen. Daarmee vervullen API

gegevens een rol bij de bestrijding van mensenhandel of –smokkel. Het gebruik van API draagt hiermee bij aan een effectievere grenscontrole.

Kanttekeningen bij het gebruik van API

Onderzoeksvraag 6 gaat over wat er goed gaat en beter kan met het gebruik van API in de praktijk. De kanttekeningen die we hebben geven hierop een antwoord. Een eerste kanttekening is dat er ruimte bestaat tussen het aantal passagiers waarvoor het API-Centrum een alert doet uitgaan en het aantal dat daadwerkelijk aan de grens wordt staande gehouden voor een aanvullend gesprek of onderzoek. Met andere woorden: een deel van de alerts wordt niet opgevolgd door een gesprek met de gesignaleerde passagier of een nader onderzoek.

De KMar verklaart dit onder andere met het gegeven dat niet elke passagier waarvoor een alert wordt verstuurd ook daadwerkelijk een grensdoorlaatpost passeert. Passagiers die doorreizen naar een volgende bestemming via Schiphol reizen worden niet in alle gevallen in Nederland opgevolgd. Alerts met een hoog risico op inbreuk op de veiligheid in Nederland of Schengen worden in beginsel allemaal opgevolgd, bijvoorbeeld met de inzet van DGC medewerkers. In 2017 is circa 37% van de passagiers op Schiphol[33] doorgereisd naar een andere bestemming. Het komt ook incidenteel voor dat alerts niet worden opgevolgd vanwege storingen in de systemen, de nachtelijke uren of een tekort aan capaciteit.

Het is daarnaast niet uit te sluiten dat door de huidige schriftelijke doorgifte aan de doorlaatposten, alerts niet altijd worden opgevolgd. De huidige manier van werken vergt veel van de oplettendheid van de grenswachten. Zij moeten de passagiers die op de A4'tjes staan vermeld in hun achterhoofd houden. Op basis van de gesprekken die zijn gevoerd tijdens het meelopen in de operatie gaat het gemiddeld om 5 A4'tjes. Hoewel de gesproken KMar-medewerkers verschillen in hun inschatting van hoeveel gesignaleerde passagiers er met deze werkwijze niet worden gezien, bestaat er wel een breed gedragen wens naar een adequate voorziening om alerts aan de grens te krijgen. Over het algemeen wordt dit gezien als een wenselijk sluitstuk op het voorgestane geautomatiseerd en informatie gestuurd grensbeheer. Het vereist wel dat voortaan van elke passagier het reisdocument gescand moet worden en dat kan enige tijd vragen afhankelijk van de beschikbare techniek en snelheid van databases. KMar geeft aan dat zo'n systeem in het eerste kwartaal van 2019 operationeel wordt.

Een tweede kanttekening kan worden geplaatst bij de verwerkingen door het API-Centrum. Kijkend naar de alerts die de afgelopen jaren zijn verstuurd dan blijkt het leeuwendeel betrekking te hebben op directe matches. Vooralsnog worden door het API-Centrum vooral de passagiers eruit gehaald die in een opsporingsregister of op een watchlist staan. Van de in totaal 11.082 alerts die in 2017 werden gedaan, hadden er 6.710 (60,5%) betrekking passagiers die stonden geregistreerd vanwege een misdrijf of overtreding. Omvangrijk is de als bijvangst te

[33] Feiten&Cijfers 2017, Schipholgroep

beschouwen groep alerts waarin melding wordt gedaan van een Mulderfeit (boetes die verband houden met verkeersovertredingen).

Kijkend naar de inhoud van de alerts kan worden vastgesteld dat het aantal alerts dat betrekking heeft op (een risico op) illegale immigratie uitkomt op 421 in 2017. Op basis van de watchlist zijn in 2017 49 contraterrorisme 'subjects' in beeld gekomen. De watchlist is hiermee een duidelijke aanvulling op OPS en SIS. Het aantal alerts dat betrekking heeft op 'unknown persons with an unknown risk' op basis van handmatige beoordelingen en profielen komt uit op 2.322 in 2017.

Er is op dit moment nog geen sprake van een gesystematiseerde of geautomatiseerde screening aan de hand van algoritmes. Binnen het API-Centrum en de Sectie A&O bestaat de wens om dit verder te ontwikkelen.

In het eerste kwartaal van 2018 is van 40% van alle alerts geen terugkoppeling ontvangen. Over heel 2017 is dat bij 60% van de alerts het geval. Goede terugkoppelingen zijn van belang om de effectiviteit van de alerts te monitoren en goede analyses te maken voor het verder ontwikkelen van profielen en algoritmes.

Tijdens het onderzoek zijn geen duidelijke onverwachte effecten van het API-gebruik naar voren gekomen (vraag 11). Hooguit is er sprake van 'bijvangst': door de API-procedures hebben luchtvaartmaatschappijen sneller een complete API-batch ter beschikking. In geval van een calamiteit met een vlucht is daardoor snel een volledige passagierslijst beschikbaar. Een bijvangst is ook de detectie van de Mulderfeiten. API is immers niet primair ingevoerd om dit soort zaken aan de grens te detecteren.

In het onderzoek hebben we geen andere factoren naast het gebruik van API dan de besproken ontwikkelingen ontdekt die van invloed zijn op het verbeteren van de grenscontrole en/of het bestrijden van illegale immigratie (onderzoeksvraag 9).

API in het licht van toekomstige ontwikkelingen

De vragen 13 en 14 gaan over Europese ontwikkelingen en de impact daarvan op het gebruik van API-gegevens. Zoals beschreven in het tweede hoofdstuk is de API-richtlijn een onderdeel en zelfs de eerste bouwsteen van een breder pakket van Europese maatregelen en plannen om de buitengrenzen te versterken. API was hierin de eerste stap. De functie en meerwaarde van API-gegevens wordt door deze ontwikkelingen beïnvloed. Met name twee ontwikkelingen zijn relevant: de komst van EES en ETIAS en de op handen zijnde verplichting voor luchtvaartmaatschappijen om ook PNR-gegevens te verstrekken voor vluchten van buiten en binnen Schengen. Daarmee kunnen de autoriteiten over meer gegevens beschikken en ook beter de vervoersbewegingen van mensen volgen. Een ander effect is dat autoriteiten binnen Europa nog meer moeten samenwerken om elkaars bestanden te kunnen raadplegen en te vergelijken met de gegevens van de passagiers.

In het kader van de ontwikkeling van ETIAS wordt het voor luchtvaartmaatschappijen belangrijker om eerder over betrouwbare passagiersgegevens te beschikken dan het 'first point of contact' met de passagier op de luchthaven vlak voor de vlucht. ETIAS is een soort visum voor niet-visumplichtigen. Zonder ETIAS-reisautorisatie mag een niet-visumplichtige derdelander niet aan boord.

Luchtvaartmaatschappijen zullen zoveel mogelijk willen voorkomen dat pas bij het boarden duidelijk wordt dat een passagier moet worden geweigerd. Zij zullen daarom al bij hun ticketverkoop om ETIAS- en API-gegevens vragen, zodat zij passagiers die geen autorisatie hebben (omdat zij dat nog niet hebben aangevraagd of omdat die hen is geweigerd) tijdig kunnen informeren. In dit licht is het aannemelijk dat structureel gebruik zal worden gemaakt van 'ongevalideerde API-gegevens' ofwel API-gegevens die door de passagier zelf worden ingevuld en door de vervoerder worden gebruikt nog voordat de vervoerder deze heeft kunnen valideren. Autoriteiten in het bestemmingsland krijgen dan eerder de beschikking over alle gegevens en kunnen de analyses al uitvoeren. Bij het boarden kan er dan na het uitlezen van het reisdocument via een interactieve verbinding een signaal komen of de passagier aan boord mag of niet.

Hoewel de API- en PNR-verplichting van elkaar verschillen en met een ander doel zullen worden opgelegd aan luchtvaartmaatschappijen, is met voorliggende evaluatie duidelijk geworden dat de verschillen in de praktijk voor luchtvaartmaatschappijen nu al niet altijd scherp zijn. Dat geldt zowel voor de doelbinding, de samenstelling van de datasets als voor de kwaliteit van de gegevens en de bewaartermijn.

Luchtvaartmaatschappijen vragen zich ook af wat de bewaartermijn wordt van de verstrekte gegevens. Het Vreemdelingenbesluit schrijft ten aanzien van de bewaartermijn voor API gegevens vernietiging binnen 24 uur voor als het gaat over de gegevens die de KMar ontvangt. De KMar kan in bepaalde omstandigheden data 36 uur bewaren en zelfs tot 5 jaar onder de Wpg. In het PNR-wetsvoorstel wordt een bewaartermijn genoemd van 5 jaar. Passagiersgegevens waaruit rechtstreeks de identiteit van een persoon kan worden afgeleid worden na zes maanden gedepersonaliseerd door afscherming van die gegevens. De geïnterviewde luchtvaartmaatschappijen gaan ervan uit dat op hun PNR-gegevens (waaronder API-gegevens) de AVG van toepassing is en dat zij deze derhalve meerdere jaren mogen bewaren.

Doelbinding. Daar waar API-gegevens op basis van de API-richtlijn louter mogen worden gebruikt ten behoeve van het tegengaan van illegale immigratie en het verbeteren van de grenscontrole, mogen PNR-gegevens op basis van de PNR-richtlijn (straks) louter gebruikt worden ten behoeve van de bestrijding van terroristische en ernstige misdrijven. De evaluatie beschrijft hoe API-gegevens worden gebruikt door de grensautoriteiten voor grenscontrole conform de Schengen grenscode en het tegengaan van illegale migratie. De API-gegevens helpen bij strafrechtelijke opsporing en het innen van boetes. Dat geldt zelfs voor

het leeuwendeel van de API-alerts. Een klein deel van de alerts heeft betrekking op mensen die zich (mogelijk) schuldig maken aan illegale immigratie. Het merendeel van de alerts gaat over mensen met openstaande (bestuurlijke) boetes en mensen die gezocht worden in verband met een misdrijf.

Samenstelling van de datasets. Bij PNR gaat het om passagiersgegevens die luchtvaartmaatschappijen voor hun eigen bedrijfsdoeleinden verzamelen. De PNR-dataset bevat dus altijd ook API-data voor vluchten van buiten Schengen. Het API-deel verzamelen de maatschappijen omdat dit een verplichting is vanuit de API-richtlijn zoals die in Nederland en veel andere landen is ingevoerd. Deze overlap roept bij de geïnterviewde luchtvaartmaatschappijen de vraag op waarom API en vervolgens PNR (waartoe ook API-gegevens behoren) door luchtvaartmaatschappijen gescheiden van elkaar moeten worden aangeleverd. Dat is nu al het geval voor de verplichtingen rond passagiersgegevens die de Douane oplegt. Die vraag komt vooral op omdat in een aantal niet EU-landen de gegevens via één loket worden aangeleverd.

Kwaliteit van de gegevens. Daar waar in het kader van de API-richtlijn luchtvaartmaatschappijen verantwoordelijk worden gehouden voor de juistheid van de API gegevens, kunnen zij in het kader van de PNR-wet volstaan met gegevens die door de passagier zijn verstrekt. Luchtvaartmaatschappijen hoeven die PNR niet op juistheid te controleren. Er wordt van uitgegaan dat luchtvaartmaatschappijen zelf de API-gegevens uit een paspoort overnemen (bij de check-in of bij het boarden). Deze evaluatie leert dat dat niet altijd het geval is en dat API gegevens vaak door passagiers zelf worden ingevoerd op het moment dat zij een vlucht boeken of online inchecken. De reden hiervan is dat luchtvaartmaatschappijen ruim voor het boarden over API-gegevens willen beschikken. Bijvoorbeeld omdat dat bij andere bestemmingen, zoals de Verenigde Staten, nodig is en ze daarom dezelfde werkwijze hanteren ook voor vluchten naar Nederland. API-gegevens zijn daardoor in de praktijk niet per definitie gevalideerd en onderscheiden zich daardoor minder van de persoonsgegevens uit de PNR set.

API-gegevens worden conform de doelbinding alleen gebruikt voor inreizende passagiers. Als passagiersgegevens worden gebruikt bij uitreizen, wat nu met API-gegevens nog niet het geval is, kunnen niet-EU-passagiers systematisch worden gecontroleerd op hoe lang zij aaneengesloten in het Schengengebied zijn geweest. Het is niet-visumplichtige derdelanders toegestaan voor maximaal 90 dagen binnen het Schengengebied (inclusief Zwitserland) te verblijven[34]. Nu kunnen die reizigers alleen gesignaleerd worden door de analyse van de datumstempels in paspoorten en dat kost relatief veel tijd en is bovendien foutgevoelig. API gebruiken bij uitreizen maakt het ook mogelijk reizigers die voorkomen in registers (OPS, SIS) te signaleren bij uitreizen. Mogelijke verdere meerwaarde van het gebruik van API gegevens bij uitreizen zijn niet in het onderzoek naar boven gekomen.

[34] https://ind.nl/kort-verblijf

De verwachting, en zeker bij de luchtvaartmaatschappijen ook de wens, is dat op de langere termijn 1 loket 'a single window' voor het aanleveren van passagiersgegevens een wereldwijd toegepast model wordt. In verschillende landen is dat nu al het geval. In Nederland wordt nu onderzocht of zo'n single window ook kan worden ingevoerd. De API-verplichtingen zijn nu in Nederland opgenomen in de Vreemdelingenwet en gelden ook voor Nederlandse passagiers. Naast de stroom API-passagiersgegevens krijgt de Douane in Nederland nu al de PNR-gegevens. Als de PNR-wet wordt aangenomen mogen aangewezen Bevoegde Instanties de PNR gegevens vorderen bij Pi-NL om te gebruiken voor het bestrijden van ernstige criminaliteit en terrorisme. Het inbedden van de API- en PNR-verplichtingen in één kaderwet die ziet op passagiersgegevens is in onze ogen als logische route voor de toekomst. Dit zou zeker helpen om de transparantie voor alle partijen te verhogen.

Literatuur

Wetgeving

EC DG Justice. (2006). *Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data.*

European Parliament. (2008). *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of PNR for law enforcement purposes.* B6-0615/2008.

Europese Commissie. (2004). *Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven.*

Europese Commissie. (2016). *Richtlijn (EU) 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit*.

Europese Commissie. Verordening van het Europees Parlement en de Raad tot instelling van een Europees systeem voor reisinformatie en -autorisatie (ETIAS) en tot wijziging van de Verordeningen (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/794 en (EU) 2016/1624

ICAO, *Guidelines on Passenger NameRecord (PNR) Data*, 2010

Memorie van Toelichting. (vergaderjaar 2006-2007, 30897). *Aanpassing van de Vreemdelingenwet 2000 aan richtlijn nr. 2004 /82 EG van de Raad van 29 april betreffende de verplichting voor vervoerders om passagiersgegevens door te geven.* Tweede Kamer der Staten Generaal.

Memorie van Toelichting. (Vergaderjaar 2017-2018, 34861). *Regels ter implementatie van richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische mis.* Tweede Kamer der Staten Generaal.

Minister van Vreemdelingenzaken en Integratie, e. (2006). *Plan van Aanpak Grenscontroles, Gebruik van grenscontroles bij Terrorismebestrijding.* TK 30315 nr.3.

Ministerie van Justitie. (2009). Kaderdocument Grenstoezicht - Gebruik van grenscontroles bij terrorismebestrijding. TK 30315, nr. 8.

Nota van Toelichting. (Jaargang 2012). *Besluit van 20 december 2012, houdende wijziging van het Vreemdelingenbesluit 2000 in verband met de uitbreiding van de vooraf door de luchtvervoerder te verstrekken passagiersgegevens (standaard API-set).* Tweede Kamer de Staten Generaal 688.

Staatscourant. (15 maart 2012). Richtlijn voor strafvordering strafrechtelijke aansprakelijkheid voor het verstrekken van passagiersgegevens door luchtvaartmaatschappijen.

WCO/IATA/ICAO. (2014). *Guidelines on Passenger Information.* Brussels.

Literatuur

Algemene Rekenkamer. (2005). *Gebruik van grenscontroles bij terrorismebestrijding.* Den Haag: TK 30315 nr. 2.

Brouwer, E. (2009). *The EU Passenger Name Record System (PNR) and Human Rights, Transferring Passenger Data or Passenger Freedom.* Centre for European Policy Studies, Working Document No. 320.

Brouwer, E. (2017). International cooperation and the exchange of personal data: safeguarding trust and fundamental rights. In S. Carrera, & V. Mitsilegas, *Consitutionalising the Security Union* (pp. 73-86). Brussels: Center for European Policy Studies.

Canetta, E., Korpelainen, S., Mortera, C., Robson, L., Minkova, V., & Damianakis, K. (2012). *Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82.* Brussels: ICFGHK, Milieu.

Casagran, C. (2015). The Future EU PNR System: Will Passenger Data be Protected? *European journal of crime, criminal law and criminal justice*, 241-257.

Gerritse, R. (2007). *Rapport Werkgroep Passagierscontrole Schiphol.* Den Haag: Interdepartmentale werkgroep.

Goedvolk, M. (ea), Ketenbrede impactanalyse Pi-NL Keteneffecten van de invoering van de Passagiersinformatie-eenheid Nederland, februari 2018

IATA (2017), EU Smart Borders Package Entry-Exit System, position paper / ETIAS / API, januari 2017.

IATA (2017), Revision of API directive, posion paper, 29 augustus 2017

IATA (2013) Advance Passenger Information Guidelines WCO/IATA/ICAO Passenger List Message (PAXLST) implementation guide.

Ministerie van Veiligheid en Justitie. (2013). *Evaluatierapport inzake het gebruik van Advance Passenger Information (API) in Nederland.* Den Haag.

Ministerie van Veiligheid en Justitie. (2013). *Internationaal gebruik van passagiersgegevens, een inventarisatie op hoofdlijnen.* Den Haag.

Schoenmakers, Y., De Groot, I., Van Zanten, J., Van Rooyen, A., & Baars, J. (2017). *De onvindbaren, Op zoek naar voortvluchtige veroordeelden in Nederland.* Apeldoorn: Politie en Wetenschap.

Scholten, S. (2014). *Privatisation of Immigration Control? A socio-legal Study on the Role of Private Transport Companies in The Netherlands and the United Kingdom (proefschrift).* Nijmegen: Brill/Nijhof.

Sietsma, R. (2007). *Gegevensverwerking in het kader van opsporing, Toepassing van datamining ten behoeve van de opsporingstaak, afweging van het opsporingsbelang en het recht op privacy.* Leiden: Proefschrift.

Bijlage 1 Begrippenlijst

Advance Passenger Information (API)	Advance Passenger Information een combinatie van persoonsgegevens uit het paspoort en vluchtgerelateerde informatie. Er bestaan internationaal overeengekomen richtlijnen van ICOA/IATA die bepalen welke gegevens API (maximaal) bevatten. In de Nederlandse Vreemdelingebesluit (art 2.2a) is aangegeven dat het gaat om: nummer en de aard van het reisdocument, nationaliteit, volledige naam, geboortedatum, geslacht, staat van afgifte van het reisdocument, vervaldatum, vluchtnummer, tijdstip van vertrek en aankomst van het vervoersmiddel, aantal met dat vervoermiddel vervoerde passagiers, grensdoorlaatpost van binnenkomst, eerste instappunt, overige reisroutegegevens, Passenger Name Record-bestandslocatie.
Alert	Onder een alert wordt verstaan een hit waarvoor een interventieopdracht genaamd alert is verzonden.
API-Centrum	Onderdeel van het Targeting Center Borders van de KMar dat op basis van API-gegevens API-alerts afgeeft
Arinc	Private onderneming die uiteenlopende diensten levert op luchtvaartgebied; fungeert o.a. als provider van door luchtvaartmaatschappijen aangeleverde data en bewerkt deze data tot het juiste format.
Dedicated Gate Control (DGC)	DGC is onderdeel van de KMar op Schiphol dat gespecialiseerd is in het uitvoeren van controles aan de gate. Het zijn mobiele teams die op basis van een API-alert een gesignaleerde passagier aan de gate kunnen opwachten.
Entry-Exit Systeem (EES)	Dit systeem dat uiterlijk 2020 in werking moet zijn, moet de gegevens gaan registreren inzake inreis, uitreis en weigering van toegang van onderdanen van derde landen die de buitengrenzen van het Schengengebied overschrijden.
European Travel Information and Authorisation System (ETIAS)	Op dit moment wordt gewerkt aan een European travel information and authorisation system (ETIAS). Het is een systeem waarmee niet-visumplichtige onderdanen van derde landen, voor hun afreis online een reisautorisatie moeten aanvragen. De in de aanvraag ingevulde informatie wordt aan de hand van EU-databanken en relevante Interpol-databanken verwerkt om na te gaan of er gronden tot weigering van een reisautorisatie zijn.
Grensbeheer	Alle activiteiten gericht op het tegengaan van illegale immigratie en de aanvoer van ongewenste

	goederen en het bestrijden van grensoverschrijdende criminaliteit, hetzij op een doorlaatpost, hetzij in het kader van de uitvoering van patrouilles of surveillance. Grensbeheer kan dermate breed worden opgevat dat ook inspanningen van andere dan grensautoriteiten kunnen worden geschaard zoals bijvoorbeeld controle op illegale arbeid door de Inspectie SZW. Ook kunnen er inspanningen van private partijen toe worden gerekend de inspanningen van luchtvaartmaatschappijen in het kader van hun carrier liability.
Grenscontrole	Daadwerkelijke controle van personen op een grensdoorlaatpost, of tijdens surveillance, aan een buitengrens van het Schengengebied.
Hit	Onder een hit wordt verstaan een gevalideerde match, dat wil zeggen een match ten aanzien waarvan een verificatie heeft plaatsgevonden, bijv. vergelijking met een actuele database. Onder een no-hit wordt verstaan: gegevens die geen match hebben opgeleverd dan wel waarvan de match na validatie niet als hit is aangemerkt.
International Air Transport Association (IATA)	IATA vertegenwoordigd op dit moment 290 luchtvaartmaatschappijen, die tezamen ruim tachtig procent van het luchtverkeer voor hun rekening nemen.
International Civil Aviation Organization (ICAO)	International Civil Aviation Organization is een gespecialiseerde organisatie van de Verenigde Naties. ICAO heeft tot doel principes en standaarden voor de Internationale burgerluchtvaart op te stellen ter verbetering van het luchtverkeer. Aan ICAO nemen op dit moment 191 staten deel.
Machine Readable Zone (MRZ)	Identiteitsdocumenten zoals paspoorten en ID-kaarten bevatten -naast de gegevens van houder- een Machine Readable Zone (MRZ). Dit zijn de twee of drie regels onderaan het voorblad van het paspoort of aan de achterkant van een ID-kaart. In de MRZ zijn gegevens opgenomen welke ook elders geprint staan op het document zoals naam en voornamen, geboortedatum, dag van uitgifte en geldigheid, documentnummer, nationaliteit, land van uitgifte et cetera. Naast deze gegevens bevat de MRZ een aantal controlegetallen, hiermee is te berekenen of de data in de MRZ klopt. Dit heeft tot voordeel dat de MRZ lastiger vervalst kan worden.
Match	Van een match is sprake wanneer persoonsgegevens (zoals API) overeenkomen met de gegevens van personen die voorkomen op een watchlist/database of de indicatoren van een risicoprofiel.
Mulderfeit	Verkeersoverredingen die volgens het bestuursrecht worden afgedaan.

Opsporingsregister (OPS)	Het Opsporingsregister (OPS) is de aanduiding van het register waarin zaken van personen met een openstaande vrijheidsstraf zijn opgenomen. Het is een Nederlands register. In het OPS zijn geen zaken opgenomen die onder het reguliere proces van tenuitvoerlegging, oftewel de werkvoorraad, vallen. (Schoenmakers, De Groot, Van Zanten, Van Rooyen, & Baars, 2017)
Passenger Name Record (PNR)	Deze gegevens worden vastgelegd bij het boeken van een reis. In bijlage 4 is weergegeven welke gegevens in de PNR-set zijn opgenomen.
Programma Vernieuwing Grensmanagement (VGM)	Het programma VGM is medio 2008 van start gegaan met als doelstelling de ambitie van de Nederlandse overheid op het gebied van de vernieuwing van het grensmanagement vorm te geven en tegelijkertijd invulling te geven aan het kabinetsbeleid voor het behoud van de positie van Schiphol als één van de belangrijkste 'hubs' (knooppunten van verbindingen) in Noordwest Europa.
Schengen Informatie Systeem -tweede generatie (SISII)	Een Europese database die Europese landen faciliteert ten behoeve van strafrechtelijke opsporing, handhaving van immigratie wetgeving en grenscontrole. Met SISII wisselen landen real time informatie uit onder andere over: • Personen om wier aanhouding ter uitlevering wordt gevraagd, • Vreemdelingen die de toegang tot het Schengengebied geweigerd moet worden, • Vermiste personen, • Personen van wie de verblijfplaats moet worden vastgesteld, • Personen die onopvallend hetzij gericht gecontroleerd moeten worden, • Vermiste minderjarigen met verzoek tot opsporing en terugbrenging, • Personen die reizen op blanco of op naam gesteld identiteitsbewijzen die als gestolen vermeld staan.
Stolen and Lost Travel Documents Database (SLTD)	Stolen and Lost Travel Documents Database, een register waar alleen reisdocumenten in staan gesignaleerd die niet meer in bezit zijn van de rechtmatige houder. Het zijn documenten die door de houder als vermist zijn opgegeven. Het register is in 2002 door Interpol opgezet en wordt gevoed door de landen die bij Interpol zijn aangesloten.
Targeting Centre Borders (TCB)	TCB is een onderdeel van de KMar waar personen worden gesignaleerd die van buiten de EU naar Nederland reizen die gecontroleerd moeten worden, ofwel omdat zij voorkomen op een watchlist ofwel omdat zij voldoen aan een risicoprofiel. Het TCB bestaat uit 5 eenheden: de Eenheid Watchlisten en Profielen, het API-Centrum (commerciële luchtvaart), de Maritieme Backoffice (water), Bureau

	Targeting Land (land) en General Aviation Backoffice (kleine burgerluchtvaart).
Travel Information Portal (TRIP)	Sinds 2016 vindt de aanlevering van reisgegevens aan de Douane plaats via een beveiligd portaal. Dit is het Travel Information Portal (TRIP).
Watchlist	Een lijst die één of meerdere karakteristieken bevat van één of meerdere personen of objecten. De watchlist wordt door bevoegde instanties samengesteld en door tussenkomst van de Officier van Justitie aangeleverd. De watchlist heeft een nationale status en kan alleen door Nederlandse autoriteiten worden bekeken.
World Customs Organization (WCO)	WCO is een onafhankelijk intergouvernementeel samenwerkingsverband van douaneautoriteiten ter bevordering van hun effectiviteit en efficiëntie.

Bijlage 2 Cijfermatig overzicht

Ten behoeve van deze evaluatie heeft de KMar overzichten verstrekt van aantallen matches, hits en alerts die vanaf 2013 zijn gevonden c.q. afgegeven.

- Match: Een match wil zeggen dat de data-kenmerken overeenkomen met de data-kenmerken die voorkomen op een watchlist/database of een risicoprofiel.
- Hit: Onder een hit wordt verstaan een gevalideerde match, dat wil zeggen een match waarbij een verificatie op naam en/of persoonsgegevens heeft plaatsgevonden. Dat kan bijvoorbeeld door vergelijking met actuele databases en via een check op actualiteit van de signalering. Een hit kan worden verrijkt met additionele gegevens. Bijvoorbeeld specifieke bejegeningsgegevens en/of foto. Een hit leidt niet altijd tot een interventiebericht: een alert. Het kan ook een administratieve melding zijn aan de eigenaar van de Watchlist of Profiel opgenomen in het API3-systeem
- Alert: Onder een alert wordt verstaan een hit ten aanzien waarvan een interventieopdracht genaamd alert is verzonden.

De verhouding tussen matches, hits en alerts ten opzichte van het aantal passagiers is omgerekend naar een percentage. De absolute aantallen zijn tussen de verschillende jaren namelijk niet te vergelijken. Pas vanaf juni 2016 is het voor vluchten vanaf alle luchthavens buiten Schengen naar Nederland verplicht API-gegevens aan te leveren. De resultaten zijn te zien in figuur 6. De lijn van het percentage matches ten opzichte van het aantal passagiers is grillig voor de periode 2013 tot september 2016. Vanaf september 2016 is het percentage redelijk stabiel binnen de marge 0,5% en 0,8%. Hits en alerts zijn over de hele meetperiode stabiel rond 0,1%. De KMar schrijft dit verloop van de fractie matches toe aan verbeteringen die zijn doorgevoerd in de verschillende watchlists. Daarnaast is er een leercurve doorlopen rond het gebruik van opsporingsprofielen en handmatige beoordelingen.

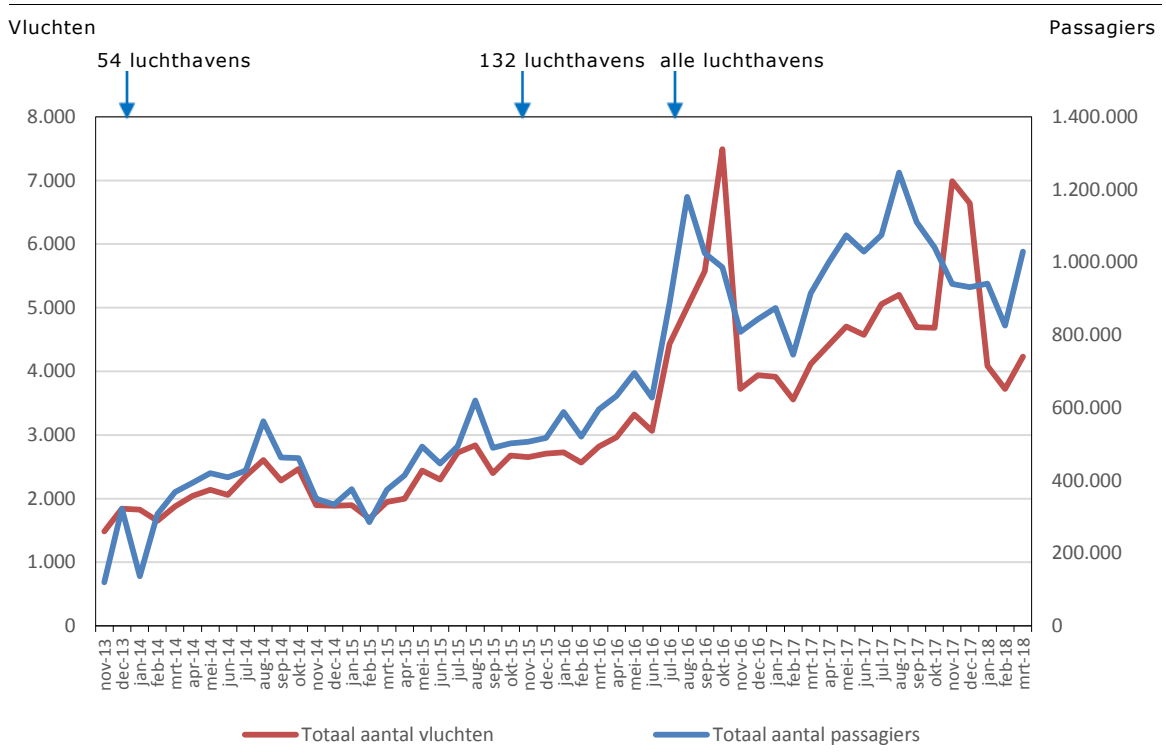
Het verschillen tussen matches en alerts is direct het gevolg van de werkzaamheden van het TCB. Veel matches komen naar voren omdat niet alleen op een 100% match van passagiers gegevens wordt gekoppeld. Ook varianten worden gebruikt. Daarmee komen passagiers naar boven als matches die een vergelijkbare naam hebben. TCB zoekt vervolgens uit welke match de passagier is die op basis van de bestanden degene is die nadere aandacht moet krijgen. Op die manier vallen veel matches af.

Voor deze evaluatie zijn de tellingen per maand gebruikt per luchthaven. Het is niet mogelijk om hiermee individuele gevallen te volgen om zo te kunnen analyseren welke soort matches een hit/alert zijn geworden, welke zijn opgevolgd en wat de terugkoppeling is van die hits/alerts. Daardoor is het niet mogelijk op basis van de data te verklaren of beschrijven waarom welke hits/alerts wel en welke niet worden opgevolgd. De terugkoppeling van alerts is niet volledig en de fractie

waarover een terugkoppeling beschikbaar is in de database verschilt per jaar.

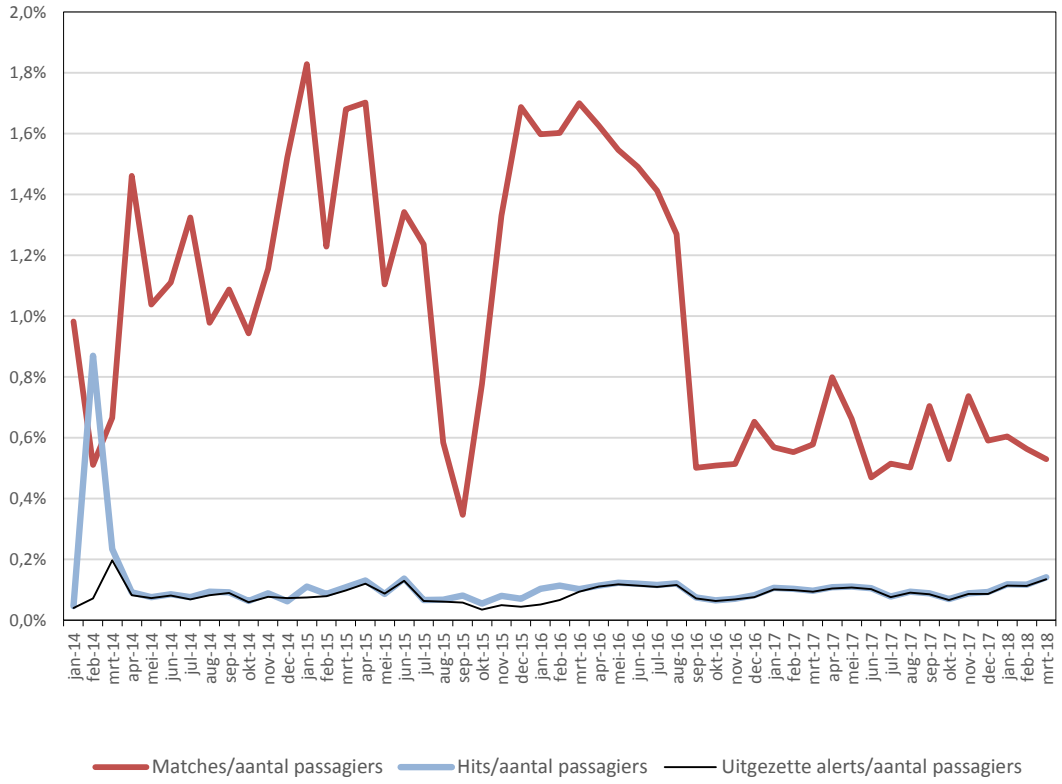
Op basis van de aangeleverde cijfers is in kaart gebracht hoe het aantal vluchten waarvoor de API-verplichting van toepassing is zich heeft ontwikkeld. Het aantal passagiers is ter vergelijking in figuur 5 afgebeeld. Een duidelijke piek is te zien na juni 2016. Vanaf dat moment is het verplicht om vanaf alle luchthavens van vertrek buiten Schengen de API gegevens aan te leveren. Daarvoor was dat voor 54 luchthavens het geval. Het gemiddelde aantal passagiers per vlucht is ruim 200.

figuur 5 Aantal API-plichtige vluchten en passagiers in de periode 2013-2018



Bron: KMar

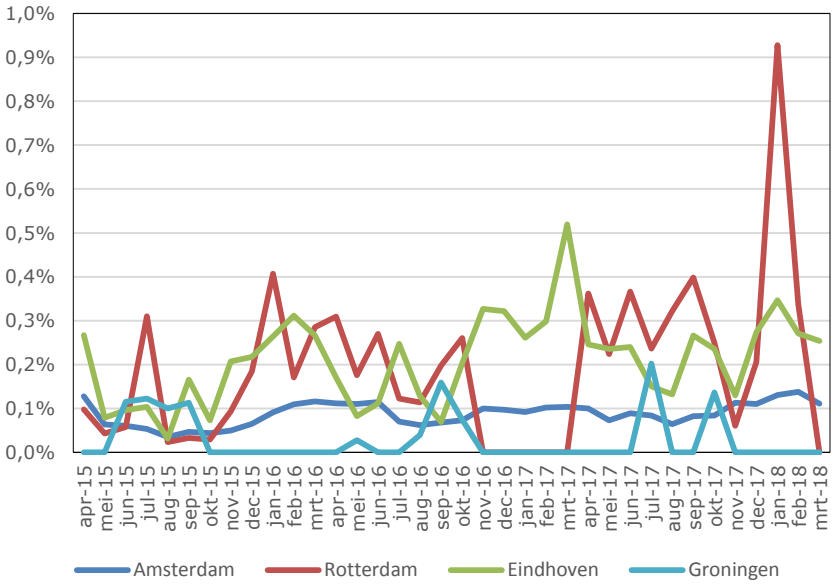
figuur 6 Kengetallen: percentage matches, hits en alerts t.o.v. totaal aantal passagiers



Bron: KMar

Uit de gegevens per luchthaven van aankomst blijkt dat Schiphol een zeer stabiele fractie alerts kent ten opzichte van het aantal passagiers. Deze gegevens zijn weergegeven in figuur 7 .
Schiphol is overigens goed voor ruim 95% van alle passagiers die van buiten Schengen naar Nederland reizen.

figuur 7 Alerts in procenten van aantal passagiers per luchthaven[35]



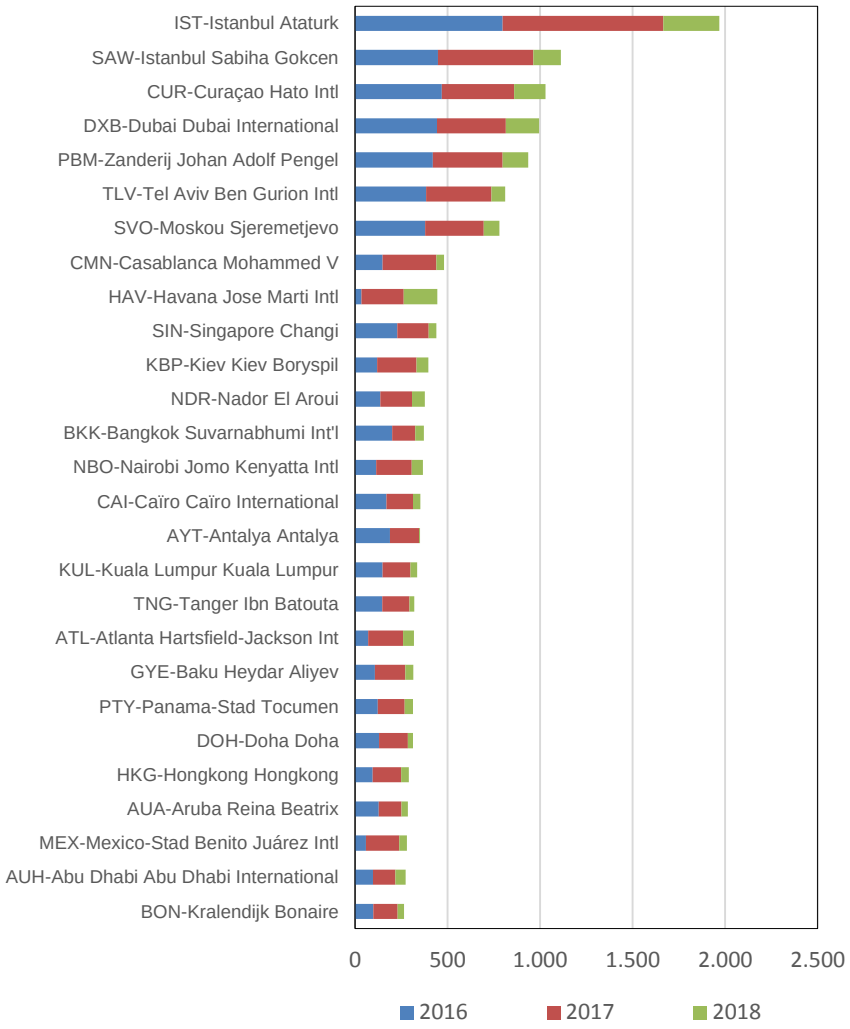
Bron: KMar

Uit de databestanden is niet voor alle jaren te achterhalen wat de luchthavens van vertrek waren van de passagiers die op de alertlijsten zijn gekomen. Voor 2016 en 2017 is dit overzicht er wel en ook voor de eerste drie maanden van 2018. In figuur 8 zijn de luchthavens van vertrek afgebeeld waarbij in deze periode in totaal meer dan 250 alerts zijn aangemaakt. Istanbul Ataturk is veruit de meest voorkomende luchthaven met op afstand de tweede luchthaven van Istanbul Sabiha Gokcen.

Voor de luchthaven Havanna valt op dat 2018 in ieder geval in het eerste kwartaal een piek laat zien: in het eerste kwartaal zijn er al 182 passagiers op de lijst gekomen, in heel 2017 ging het om 228 mensen.

[35] Voor Maastricht waren over slechts enkele maanden data beschikbaar, deze luchthaven is daarom uit de grafiek gelaten.

figuur 8 Luchthaven van vertrek in aantal alerts, 2018 alleen 1e kwartaal



Bron: KMar, landencodes via IATA-lijst aangevuld

OPS en SISII zijn de belangrijkste registers waar alerts uit voortkomen. Bijna de helft van de alerts wordt uitgezet vanwege zogenaamde Mulderfeiten (verkeersovertredingen die volgens het bestuursrecht worden afgedaan). Vanaf 2015 hebben verder veel alerts betrekking op vermiste of als gestolen gesignaleerde documenten. In tabel 6 zijn de redenen van de alerts uitgesplitst. In vetgedrukt de alerts waarbij het gaat om toegangsweigeringen.
Het detailniveau van de reproduceerbare registraties over 2013 is niet volledig. Veranderingen in de systemen zijn hiervan de oorzaak.

tabel 6 Reden versturen alerts, 2018 alleen 1e kwartaal

Bron	*Omschrijving*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*
Expertise centrum Mensensmokkel Mensenhandel (EMM)		0	1	1	1	0	0
Look Out	Diverse internationale look-outs	0	7	9	23	18	4
Nationale Documenten Systeem	Gesignaleerde documenten	0	0	3	1	0	0
OPS	Mulderfeit	100	1.059	960	3.167	4.164	1.498
	Opsporen Aanhouden	7	206	213	527	382	113
	Niet Onherroepelijk Vonnis	14	110	109	333	299	79
	Betekenis in Persoon	15	107	158	341	283	95
	Aandachtvestigingen	2	28	55	157	202	62
	Opsporen Aanhouden DNA afname	3	35	59	133	176	54
	Mulderfeit + gijzeling	38	330	332	534	55	1
	Gesignaleerde documenten	0	3	8	33	44	7
	Opsporen Verblijfplaats	2	15	13	50	41	17
	Ongewenst Vreemdeling	**0**	**2**	**2**	**8**	**15**	**7**
	Opsporen Aanhouden Terugbrengen	1	5	2	9	4	1
	Gijzeling	1	19	17	24	3	0
	Diverse signaleringen	0	0	1	0	0	0
	Totaal OPS	**183**	**1.919**	**1.929**	**5.316**	**5.668**	**1.934**
Schengen informatie system	Document gesignaleerd als gestolen/vermist	0	474	510	1.003	1.515	418
	Opsporen verblijfplaats	0	125	147	261	365	134
	Onopvallende Controle	0	85	129	277	449	146
	Niet tot Schengengebied toe te laten vreemdeling	**0**	**111**	**137**	**274**	**356**	**144**
	Gerichte controle	0	14	16	70	119	55
	Opsporen Aanhouden uitlevering/overlevering	0	17	28	67	59	18
	Gesignaleerde documenten	0	3	4	45	13	6
	Opsporen aanhouden terugbrengen / bescherming minderjarige	0	12	12	31	33	9
	Opsporen aanhouden voorgeleiden / overbrengen naar een veilige plaats	0	1	5	0	3	0
	Totaal Schengen informatie system	**0**	**842**	**988**	**2.028**	**2.912**	**930**
Watchlist	Onderkennen vreemdelingen die ondanks de asielstatus toch - rechtstreeks of via een buurland- terugreizen naar land herkomst.	0	5	31	200	270	31
	Diverse Watchlist via de Recherche	0	0	0	21	62	27
	Cter Subject(contraterrorisme)	0	0	0	43	49	22
	Inadmissible / Deportee	**0**	**7**	**5**	**24**	**47**	**15**
	Vreemdeling met een openstaande asiel vervolgprocedure	0	44	52	42	24	4
	Vreemdeling met ingetrokken verblijfsvergunning	0	1	2	7	12	3
	Aanzegging NL te verlaten	**0**	**1**	**1**	**2**	**3**	**21**
	Vreemdelingen met een ernstig vermoeden bestaat dat zij betrokken zijn bij oorlogsmisdrijven, misdrijven tegen de menselijkheid, ernstige commune delicten	0	0	0	4	3	1
	Totaal watchlist	**0**	**58**	**91**	**343**	**470**	**124**
Handmatige beoordeling		92	793	284	557	1.672	451
Beoordeling op basis van profielen		2	73	413	255	342	146
Totaal aantal alerts		**277**	**3.693**	**3.718**	**8.524**	**11.082**	**3.589**

Bron: KMar

Op veel alerts is geen terugkoppeling gegeven. KMar noemt de volgende redenen voor het lage aantal terugkoppelingen:

- Veel alerts hebben betrekking op passagiers die overstappen. Circa 37% van de passagiers stapt na aankomst in Schiphol[36] over op een volgende vlucht. Zij passeren op Schiphol geen grensdoorlaatpost. Zij kunnen alleen worden aangesproken/onderzocht d.m.v. inzet van DGC. API-gegevens bieden geen informatie over de eindbestemming van de passagiers.
- Boetes worden geïnd via een betaalzuil en niet meer in een systeem gemuteerd. Daardoor is er geen registratie van wat er met de alert is gedaan.
- Het was een lange tijd niet mogelijk om de 'ontvanger' op de alert toe te voegen, hierdoor kon niemand aansprakelijk worden gemaakt voor een terugkoppeling.
- Vanaf eind 1e kwartaal 2018 is het pas weer mogelijk dagelijks een export te sturen met openstaande alerts naar de chef van dienst. Daardoor wordt de volledigheid van de registraties beter.
- Er zijn wisselingen geweest met aanspreekpunten op de grensbewaking.

Er worden alerts gemist omdat er storingen in de systemen bij het API-Centrum kunnen optreden. In 2017 is dat 44 keer voorgekomen en in 2018 in het eerste kwartaal 48 keer.

Alerts kunnen worden gemist omdat vluchten aankomen in de nachtelijke uren en dan is er geen of onvoldoende capaciteit in het API-Centrum. In het eerste kwartaal van 2018 is dat 243 keer voorgekomen volgens de registraties in de database.

Een reden waardoor alerts niet kunnen worden opgevolgd heeft te maken met capaciteit bij de operatie. Dit jaar is dat 14 keer als terugkoppeling ingevoerd.

In tabel 7 zijn alle terugkoppelingen opgenomen over de jaren 2013 tot en met het eerste kwartaal van 2018. In 2014 en 2015 is als gevolg van de veranderingen in automatiseringssystemen geen volledige registratie van de terugkoppelingen beschikbaar. De Mulder-gerelateerde alerts komen het meest voor in het overzicht. In vetgedrukt de alerts waarbij toegangsweigering aan de orde is[37]. Opvallend is het deel waarvan geen terugkoppeling is ontvangen. In 2016 is dat 45%, in 2017 60% en in het eerste kwartaal van 2018 40%. De relatief grote fractie passagiers die overstappen op een andere vlucht speelt hierbij een rol.

[36] Feiten&Cijfers 2017, Schipholgroep

[37] Toelichting op tabel 5: het verschil tussen Ongewenst vreemdeling groot en klein is een interne KMar-duiding voor een artikel 67-afhandeling:
Groot heeft betrekking op iemand die geweigerd wordt op basis van een signalering en dat deze wordt vastgezet/in hechtenis genomen tot de verwijdering is geregeld en
Klein is dat geen sprake is van een signalering maar een reguliere weigering omdat niet is voldaan aan de toelatingseisen en dat de persoon via de G4 gate zelf zijn terugreis regelt.

De KMar verwacht in het eerste kwartaal in 2019 te kunnen werken met een verbeterd systeem om alerts op te volgen en daarmee ook de terugkoppeling volledig te registreren. Alle paspoorten van passagiers worden dan uitgelezen en vergeleken met de uitstaande alerts. Nu wordt nog gebruikgemaakt van uitgeprinte e-mailberichten die bij de grensdoorlaatposten liggen.

tabel 7 Terugkoppeling alerts, 2018 alleen 1e kwartaal

Terugkoppeling	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*
Totaal aantal alerts	**277**	**3.693**	**3.718**	**8.524**	**11.082**	**3.589**
Geen terugkoppeling ontvangen	**277**	**136**	**1.081**	**3.919**	**6.737**	**1.564**
Mulder buitengebruikstelling (gijzeling) geïnd	0	0	307	1.497	816	281
Gegevens vastgelegd (i.v.m. informatie verzoek)	0	0	0	51	536	153
Telling statistiek	0	0	60	486	376	184
Anders: geen specifieke omschrijving in database	0	317	101	207	371	200
Onopvallende controle	0	0	38	171	190	81
Document niet ingenomen	0	0	32	258	166	46
Administratieve alerts	0	0	1	55	165	53
Gemiste alert (i.v.m. nachtelijke uren)	0	0	1	1	160	243
Betekenis in persoon van een vonnis	0	0	61	244	159	74
Informatie verzameld en vastgelegd	0	0	59	170	140	24
Opsporen verblijfplaats	0	0	39	166	136	65
Onherroepelijk vonnis: inning	0	0	56	225	122	41
Opsporen aanhouden DNA afnemen	0	6	41	116	117	42
Doorvlucht buiten Schengen	0	0	0	0	106	216
Document ingenomen	0	0	30	67	100	51
Opsporen aanhouden	0	29	62	95	93	27
Niet onherroepelijk vonnis betekent	0	0	14	107	85	23
Onherroepelijk vonnis: aanhouding	0	0	17	173	81	23
Ongewenst vreemdeling (Klein)	**0**	**0**	**20**	**85**	**80**	**27**
Aandachtvestiging gegevens vastgelegd voor derden	0	0	26	108	73	34
Asiel aanvraag	0	6	14	36	50	14
Gerichte controle	0	0	0	33	46	30
Gemiste alert (i.v.m. storing API systeem)	0	0	0	0	44	48
Geen capaciteit	0	0	51	34	30	14
Ongewenst vreemdeling (Groot)	**0**	**0**	**10**	**17**	**20**	**13**
Toegang geweigerd	**0**	**4**	**2**	**16**	**20**	**6**
Opsporen Aanhouden Uitlevering / Overlevering	0	0	4	40	16	2
Mulder (buitengebruikstelling) gegijzeld	0	0	50	120	13	2
Opsporen aanhouden voorgeleiden	0	0	1	16	10	1
Opsporen aanhouden terugbrengen	0	0	2	4	9	4
Vals/vervalst document	0	0	1	4	8	3
Inning signalering	0	168	185	0	0	0
Mutatie gemaakt/gegevens vastgelegd	0	39	172	0	0	0
Mededeling	0	78	90	0	0	0
Gijzeling	0	7	2	0	0	0
Signalering niet (meer) van toepassing	0	3	46	0	0	0
Bleek toch niet dezelfde persoon te zijn	0	0	13	0	0	0
Ten onrechte op de alert lijst	0	0	5	0	0	0

Bron: KMar, voor 2014 en 2015 geen volledige registraties beschikbaar.

‘Telling statistiek’ in tabel 6 heeft betrekking op personen die staande worden gehouden om bijvoorbeeld een aantal openstaande boetes/vorderingen te voldoen en niet in staat zijn om daar gevolg aan te geven Dan wordt dit geregistreerd als "telling statistiek".
Het feit (reden staande houden/alert) op zich is dan onvoldoende om de persoon de toegang te ontzeggen maar de grensafhandeling heeft hierin wel tijd gestoken. Dit wordt dan als telling statistieken vastgelegd en tevens wordt op het dossier dan de aantekening gemaakt dat de persoon is aangesproken maar niet aan de vraag heeft kunnen voldoen. Hierdoor blijft de reden voor het staande houden (het gepleegde feit) ook in de lopende systemen gehandhaafd en kan hij bij een volgende aanhouding opnieuw gevorderd worden om aan de boete/vordering te voldoen.

Bijlage 3 Geïnterviewde personen

Koninklijke Marechaussee		
Naam	*Organisatie*	*Functie*
Willem Mudde	Targeting Centre Borders	Hoofd Pi-NL voormalig hoofd TCB
Robert Post	Targeting Centre Borders	plv. Hoofd TCB / senior Adviseur IND
Patrick van Doormaal	Targeting Centre Borders	Hoofd TCB
Lida Daniëls	Staf Commandant Koninklijke Marechaussee	Stafadviseur Grensmanagement
Joost Kroon	Dedicated Gate Control	Wachtmeester
Daan van der Lugt	Dedicated Gate Control	Wachtmeester
Andre Dharampal	Brigade Vreemdelingenzaken	Wachtmeester
Jorrit Greydanus	Brigade Grensbewaking	Plaatsvervangend Commandant
Linda Wiegel	Dedicated Gate Control	2e teamleider Dedicated Gate Controle (DGC)
2 personen *	Afdeling Intelligence, Sectie Analyse & Onderzoek	
Luchtvaartmaatschappijen		
Egbert-Jan van den Berge	Corendon	Manager Ground Operations
Ricard Hol	Transavia	Quality Insurance and Security
Maikel van de Ham	Transavia	Safety engineer
Gijs Harzema	Transavia	Quality Insurance and Security
Benny Mizrahi	KLM	Ground Handling Standards & Procedures Expert
Marjon Baas	KLM	Ground Handling Standards & Procedures
Brancheverteгenwoordiging		
Nuria Fermosa	IATA	Beleidsmedewerker
Ministeries		
Sander Luijsterburg	Ministerie van Justitie en Veiligheid/ Directie Migratiebeleid	Plv Hoofd Toezicht, regulier, Nationaliteit
Michael Vonk	Ministerie van Justitie en Veiligheid	Senior beleidsmedewerker/juridisch adviseur
Lou Errens	NCTV	Project manager
Diantha Raadgers	Ministerie van Infrastructuur en Waterstaat	Beleidsmedewerker / Panellid ICAO
Janneke Kolk	Ministerie van Infrastructuur en Waterstaat	Beleidsmedewerker
Kennisinstelling		
Sophie Scholten	Politieacademie	Promoveerde bij de Radboud Universiteit op een onderzoek naar de rol van private vervoerders bij grenscontrole

***** De geïnterviewden hebben aangegeven anoniem te willen blijven

Bijlage 4 API en PNR data velden

In het PNR-wetsvoorstel is de volgend lijst van datavelden opgenomen die luchtvaartmaatschappijen in het kader van de PNR-wet moeten aanleveren. Onderdeel hiervan zijn de API-gegevens. In de tabel is weergegeven welke gegevens op basis van welke grondslag moeten worden aangeleverd.

Grondslag:		
API Richtlijn/Vreemdelingenwet (KMar TCB/API-Centrum)	PNR Richtlijn (Pi-NL)	artikel 15 DWU -voorheen artikel 14 CDW- juncto artikel 1:32 ADW (Douane)
Van toepassing op:		
Inkomende vluchten van buiten de EU	Alle inkomende en uitgaande vluchten	Alle inkomende en uitgaande vluchten
Datavelden:		
PNR-bestandslocatie	PNR-bestandslocatie	PNR-bestandslocatie
	Datum van reservering/afgifte van het biljet	Datum van reservering/afgifte van het biljet
	Geplande reisdatum (-data)	Geplande reisdatum (-data)
	Naam/namen	Naam/namen
	Adres en contactgegevens (telefoonnummer, e-mailadres)	Adres en contactgegevens (telefoonnummer, e-mailadres)
	Alle betalingsinformatie, met inbegrip van het factuuradres	Alle betalingsinformatie, met inbegrip van het factuuradres
	Volledige reisroute voor dit specifieke PNR	Volledige reisroute voor dit specifieke PNR
	Informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen	Informatie betreffende reizigers die gebruikmaken van een loyaliteitsprogramma voor frequent reizen
	Reisbureau/reisagent	Reisbureau/reisagent
	Reisstatus van de passagier, met inbegrip van bevestigingen, check-in-status en „no-show” of „go-show”-informatie	Reisstatus van de passagier, met inbegrip van bevestigingen, check-in-status en „no-show” of „go-show”-informatie
	Opgesplitste/opgedeelde PNR-informatie	Opgesplitste/opgedeelde PNR-informatie
	Algemene opmerkingen (met inbegrip van alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de	Algemene opmerkingen (met inbegrip van alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de

	minderjarige, functionaris voor vertrek en aankomst)	minderjarige, functionaris voor vertrek en aankomst)
	Informatie uit de biljetuitgifte („ticketing field”-informatie), waaronder het biljetnummer, de uitgiftedatum van het reisbiljet, biljetten voor enkele reizen en geautomatiseerde prijsnotering van reisbiljetten	Informatie uit de biljetuitgifte („ticketing field”-informatie), waaronder het biljetnummer, de uitgiftedatum van het reisbiljet, biljetten voor enkele reizen en geautomatiseerde prijsnotering van reisbiljetten
	Zitplaatsinformatie, waaronder het zitplaatsnummer	Zitplaatsinformatie, waaronder het zitplaatsnummer
	Informatie over gemeenschappelijke vluchtnummers	Informatie over gemeenschappelijke vluchtnummers
	Alle bagage-informatie	Alle bagage-informatie
	Aantal en namen van de andere reizigers in het PNR	Aantal en namen van de andere reizigers in het PNR
De verzamelde API-gegevens (Advance Passenger Information): • nummer van het reisdocument • aard van het reisdocument • nationaliteit • volledige naam • geboortedatum • geslacht • staat van afgifte van het reisdocument • vervaldatum • vluchtnummer • tijdstip van vertrek en aankomst van het vervoersmiddel • aantal met dat vervoermiddel vervoerde passagiers • grensdoorlaatpost van binnenkomst • eerste instappunt • overige reisroutegegevens	De verzamelde API-gegevens (Advance Passenger Information): • nummer van het reisdocument • aard van het reisdocument • nationaliteit • volledige naam • geboortedatum • geslacht • staat van afgifte van het reisdocument • vervaldatum • vluchtnummer • tijdstip van vertrek en aankomst van het vervoersmiddel • aantal met dat vervoermiddel vervoerde passagiers • grensdoorlaatpost van binnenkomst • eerste instappunt • overige reisroutegegevens	De verzamelde API-gegevens (Advance Passenger Information): • nummer van het reisdocument • aard van het reisdocument • nationaliteit • volledige naam • geboortedatum • geslacht • staat van afgifte van het reisdocument • vervaldatum • vluchtnummer • tijdstip van vertrek en aankomst van het vervoersmiddel • aantal met dat vervoermiddel vervoerde passagiers • grensdoorlaatpost van binnenkomst • eerste instappunt • overige reisroutegegevens