Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

629

Vragen van het lid **Verhoeven** (D66) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Paspoortscanner op mobieltje vormt risico voor identiteitsfraude»* (ingezonden 17 oktober 2019).

Antwoord van Minister **Ollongren** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 5 november 2019).

Vraag 1
Kent u het bericht «Paspoortscanner op mobieltje vormt risico voor identiteitsfraude»?[1]

Antwoord 1
Ja, ik ben bekend met dit bericht.

Vraag 2
Erkent u de risico's voor identiteitsfraude die ontstaan nu er simpele telefoonapps bestaan die de chip op een paspoort kunnen scannen en uitlezen? Zo ja, wat doet u om deze risico's te minimaliseren? Zo nee, waarom niet?

Antwoord 2
Steeds meer telefoons beschikken tegenwoordig over de technologie om via NFC[2] chips uit te lezen. Met deze ontwikkeling zijn er ook apps gekomen die het uitlezen van de chip op paspoorten mogelijk maken. Het bestaan van deze telefoonapps introduceert echter geen nieuwe risico's. Bij het uitlezen van de chip zijn dezelfde persoonsgegevens zichtbaar als bij het tonen van een paspoort of het verstrekken van een kopie. Bij het verstrekken van informatie uit een paspoort moet goed worden opgelet aan wie die informatie wordt verstrekt en waarom. Dit is ongeacht of het paspoort wordt getoond, gekopieerd of gescand.
De chip in paspoorten (en identiteitskaarten) is ingericht en beveiligd volgens de internationaal afgesproken standaarden. Hierdoor kan de chip wereldwijd geraadpleegd worden voor identificatie bij bijvoorbeeld een grensovergang.

[1] FD, 16 oktober 2019
[2] NFC: «Near Field Communication» of te wel de techniek die ook bijvoorbeeld gebruikt wordt voor contactloos betalen en de ov-chipkaart.

ah-tk-20192020-629
ISSN 0921 - 7398
's-Gravenhage 2019

Daarnaast wordt de chip van paspoorten door veel overheidsinstanties geraadpleegd voor een efficiënte en foutloze verwerking van persoonsgegevens.
De chip op paspoorten kan alleen uitgelezen worden met behulp van een sleutel op basis van de machineleesbare strook (ook wel MRZ genoemd). Deze sleutel is alleen te raadplegen wanneer de MRZ zichtbaar is, daarvoor moet het document getoond of overhandigd worden. Hiermee wordt voorkomen dat deze chips door ieder willekeurig persoon van een afstand kunnen worden uitgelezen. De telefoonapps maken ook gebruik van de sleutel op basis van de MRZ om de chip te openen. De vingerafdrukken kunnen niet worden uitgelezen, die zijn extra versleuteld volgens de afspraken binnen de Europese Unie.

Vraag 3
Wat is uw reactie op het standpunt van de Autoriteit Persoonsgegevens dat het uitlezen van het burgerservicenummer (bsn) met name een risico vormt, waarbij bijvoorbeeld een bankrekeningnummer onder een valse naam geopend zou kunnen worden?

Antwoord 3
Aan alleen een burgerservicenummer (BSN) kunnen geen rechten worden ontleend. Wanneer er sprake is van identiteitsfraude zijn er meer persoonsgegevens bekend en gaat het bijvoorbeeld om de combinatie van NAW-gegevens (naam, adres en woonplaats) en/of bankgegevens. Het BSN is een administratief nummer en kan niet op zichzelf bepalend zijn voor de identificatie van personen.
In geval van het openen van een bankrekening moet een bank altijd een cliëntenonderzoek doen en als onderdeel hiervan de identiteit van de aanvrager controleren. Alle banken die in Nederland zaken doen zijn dit verplicht. Dit heeft als doel witwassen en financiering van terrorisme tegen te gaan. Deze identiteitscontrole is breder dan alleen controle op het BSN.

Vraag 4
Beschikken de app-makers na het scannen van een paspoort zelf over de paspoortgegevens? Kan op basis van dit soort scans in feite een database gemaakt worden met persoonsgegevens van Nederlanders? Ziet u hier een risico op identiteitsfraude? Zo nee, waarom niet? Zo ja, wat doet u om dit tegen te gaan?

Antwoord 4
Het is mogelijk dat app-makers op deze manier over paspoortgegevens kunnen beschikken. Net als met iedere andere app bestaat er een mogelijkheid dat de maker een database opbouwt met informatie over personen die de app gebruiken. In geval van kwaadwillenden zou dit kunnen leiden tot identiteitsfraude. Op dit moment is er bij mij geen geval van identiteitsfraude bekend als gevolg van het gebruik van een app die de chip in paspoorten scant. Vanzelfsprekend is het belangrijk dat men goed let op wat voor apps op een telefoon worden geplaatst en of het nodig is daarmee identiteitsbewijzen uit te lezen dan wel persoonsgegevens daarin op te geven.
Verwerking van persoonsgegevens moet voldoen aan de AVG. De AVG geldt ook voor partijen die apps aanbieden voor mobiele telefoons. In de gebruikersvoorwaarden moeten de app-makers dus duidelijk aangeven of en welke persoonsgegevens zij verwerken en hoe zij daarmee omgaan.
Zoals ik in mijn Kamerbrief van 30 september jl.[3] vermeldde, zie ik dat met de toename van het digitaal uitlezen van paspoorten en identiteitskaarten het niet altijd duidelijk is of het BSN wordt verwerkt of niet. Dit is vooral het geval bij de digitalisering van processen bij organisaties die persoonsgegevens uit paspoorten en identiteitskaarten verwerken voor hun administratie. Daarom heb ik bij de verplaatsing van het BSN naar de QR-code besloten het BSN ook niet in de chip terug te laten komen. De QR-code is dan de enige manier om het BSN geautomatiseerd te verwerken en er staan in de QR-code geen andere gegevens opgenomen dan het BSN. Daardoor is het duidelijker wanneer het BSN wordt verwerkt of niet. Vanzelfsprekend blijf ik ontwikkelin-

[3] Kamerstuk 25 764, nr. 121

gen op het gebied van identiteitsfraude volgen om te bepalen of er maatregelen nodig zijn.

Vraag 5
Kunt u toelichten waarom u certificering of toestemming voor het op de markt brengen van deze chiplezers niet nodig acht?

Antwoord 5
Scanapparatuur van paspoorten en identiteitskaarten wordt gebruikt bij veel verschillende instanties die personen moeten identificeren of de persoonsgegevens uit een paspoort of identiteitskaart verwerken. Voor verwerking van persoonsgegevens is de AVG leidend. Ook apps die persoonsgegevens verwerken moeten aan de AVG voldoen.
Certificering of toestemming van scanapparatuur / chiplezers betekent extra voorschriften en toezicht naast de AVG. Dit leidt tot een grote toename aan administratieve lasten die niet in verhouding staat tot het risico dat hier aan de orde is. Tot op heden heb ik geen signalen ontvangen van identiteitsfraude als gevolg van het gebruik van deze apparatuur.

Vraag 6
Hoe beoordeelt u het risico op identiteitsdiefstal bij het plaatsen van een QR-code op paspoorten? Bent u het eens met de uitspraak van Maarten Wegdam, ceo van ReadID, dat dit de kans op identiteitsdiefstal vergroot omdat het makkelijker te vervalsen is dan een chip? Zo nee, waarom niet?

Antwoord 6
De QR-code is zelf geen echtheidskenmerk, maar wel onderdeel van een identiteitskaart of een paspoort met meerdere echtheidskenmerken. Op het moment dat de QR-code wordt vervalst of gemanipuleerd komt de uitgelezen informatie niet meer overeen met de informatie op het paspoort of de identiteitskaart. Daarom ben ik het niet eens met de uitspraak dat de QR-code de kans op identiteitsdiefstal vergroot omdat een QR-code makkelijker te vervalsen is dan een chip.

Vraag 7
Wat is uw reactie op de uitspraak van Vincent Böhre van Privacy First dat een QR-code nog steeds makkelijk is uit te lezen en dat het bsn volledig moet verdwijnen van paspoorten en andere legitimatiebewijzen?

Antwoord 7
Het BSN staat op Paspoorten en identiteitskaarten, omdat BSN-verwerkende instanties wettelijk verplicht zijn te controleren of een BSN hoort bij de persoon waarvan de persoonsgegevens worden verwerkt. Het weglaten van het BSN op deze documenten verplaatst de risico's naar het alternatief dat dan gebruikt wordt om aan deze wettelijke controleplicht te voldoen.
De QR-code is bedoeld om het BSN eenvoudig en efficiënt uit te kunnen lezen door BSN-verwerkende instanties terwijl het BSN niet meer in de MRZ op de voorzijde van de houderpagina van paspoorten vermeld staat. Burgers hoeven het BSN dan niet meer onleesbaar te maken op een kopie van het paspoort wanneer het BSN niet noodzakelijk is voor de ontvangende instantie. Dit voorstel heb ik getoetst bij de Autoriteit Persoonsgegevens. De uitkomsten daarvan heb ik met uw Kamer gedeeld op in mijn brief van 30 september jl.[4]
Zoals ik in vraag 3 al opgemerkt heb kunnen aan het BSN alleen geen rechten worden ontleend. Wanneer er sprake is van identiteitsfraude zijn er meer persoonsgegevens bekend. Het volledig weglaten van het BSN draagt overigens niet bij aan de oplossing van identiteitsfraude met gegevens van paspoorten en identiteitskaarten. Identiteitsfraude is vooral het gevolg van onjuiste of onvolledig uitgevoerde identificatieprocessen. Bijvoorbeeld door de identificatie te baseren op een kopie van een paspoort. Bestrijding van identiteitsfraude moet ten eerste gezocht worden in de robuustheid van identificatieprocessen. Binnen deze processen moet voldoende aandacht zijn

[4] Kamerstuk 25 764, nr. 121

voor controle van de identiteit en de echtheidskenmerken op een paspoort of identiteitskaart.