



## Advies nr. 100/2019 van 3 april 2019

**Betreft:** adviesaanvraag betreffende een ontwerp van koninklijk besluit *tot wijziging van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten* (CO-A-2019-087)

De Gegevensbeschermingsautoriteit (hierna de "Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid op artikel 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op het verzoek om advies van de heer Pieter De Crem, Minister van Veiligheid en van Binnenlandse Zaken, ontvangen op 28/02/2019;

Gelet op de bijkomende informatie ontvangen op 15/03/2019 en op 20/03/2019;

Gelet op het verslag van de heer Willem Debeuckelaere;

Brengt op 3 april 2019 het volgend advies uit:

## **I. VOORWERP VAN DE AANVRAAG**

De wet van 25 november 2018 *houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters*, wijzigde o.a. artikelen 6 en 6ter van de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten*. Ingevolge deze wijziging zullen de nieuw uit te reiken identiteitskaarten binnenkort een digitaal beeld bevatten van de vingerafdrukken van de houder van de kaart, beeld dat elektronisch leesbaar is.

Er werd voorzien dat de Koning bij een besluit na overleg in de Ministerraad en na advies van de Gegevensbeschermingsautoriteit, de voorwaarden en nadere regels bepaalt voor het nemen van het digitale beeld van de vingerafdrukken. Het is met het oog hierop dat het koninklijk besluit van 25 maart 2003 *betreffende de identiteitskaarten*, (hierna het koninklijk besluit) wordt aangepast door het voor advies voorgelegde ontwerp van koninklijk besluit, hierna het ontwerp. Er wordt van de gelegenheid gebruik gemaakt om nog een aantal andere aanpassingen aan te brengen.

Vanuit het perspectief van gegevensverwerking verdienen de volgende punten aandacht:

- de gebruikte elektronische chip en het aanbrengen van een tweedimensionale barcode op de identiteitskaart;
- de vereiste van de voorlegging van een medisch attest van minder dan een maand oud teneinde het bewijs te leveren van de onmogelijkheid om te tekenen omwille van een fysieke of mentale handicap of ziekte (normaal moet de houder van de identiteitskaart zijn handtekening op het basisdocument zetten);
- het regelen van wie de vingerafdrukken neemt en hoe dit gebeurt;
- de omschrijving van de gevallen waarin geen vingerafdrukken op de identiteitskaart zullen worden opgenomen;
- het niet uitreiken van een identiteitskaart in geval van twijfel over de identiteit van de houder;
- de herziening van de aangifteprocedure in geval van verlies, diefstal of vernieling van de identiteitskaart.

## **II. VOORAFGAANDE OPMERKING**

De Autoriteit ontving vanwege de FOD Binnenlandse Zaken, hierna de aanvrager, ten vertrouwelijke titel zijn DPIA. In het technisch luik van het advies wordt een synthese gegeven van de risicoanalyse op basis van de informatie die deze DPIA bevat. De omstandige commentaar van de Autoriteit op de

DPIA wordt als bijlage aan dit advies toegevoegd maar zal, gelet op het vertrouwelijk karakter, niet gepubliceerd worden.

### **III. ONDERZOEK VAN HET ONTWERP**

#### **A. Rechtsgrond**

1. De afgifte van een identiteitskaart of een vreemdelingenkaart gaat gepaard met de verwerking van persoonsgegevens zoals voorgeschreven door artikel 6 van de wet van 19 juli 1991.

2. Elke verwerking van persoonsgegevens moet steunen op een rechtsgrondslag in de zin van artikel 6 AVG. Gelet op de reglementaire omkadering van de identiteitskaart en vreemdelingenkaart lijken de verwerkingen waartoe ze aanleiding geven een rechtsgrond te kunnen vinden in artikel 6.1.c) of e) van de AVG<sup>1</sup>. Het is aan de aanvrager om deze te preciseren.

3. De Autoriteit vestigt in deze context weliswaar de aandacht op artikel 6.3 AVG dat samengelezen met artikel 8 EVRM en artikel 22 van de Grondwet, voorschrijft dat regelgeving die de verwerking van persoonsgegevens omkadert, in principe minstens volgende essentiële elementen van die verwerking zou moet vermelden:

- de aanduiding van de verwerkingsverantwoordelijke;
- het doel van de verwerking;
- de types of categorieën van te verwerken persoonsgegevens;
- de betrokkenen;
- de entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt,
- de opslagperioden.

4. Er zal hierna onderzocht worden in hoeverre deze essentiële elementen terug te vinden zijn in de relevante wettelijke bepalingen en de erbij horende bepalingen van het ontwerp.

5. Opmerking: hetgeen hierna wordt opgemerkt m.b.t. de identiteitskaart geldt bij uitbreiding en analogie eveneens voor de vreemdelingenkaart.

---

<sup>1</sup> Het is uiteraard de verwerkingsverantwoordelijke zelf die het best geplaatst is om te bepalen welke rechtsgrond aansluit bij de beoogde verwerkingen van persoonsgegevens.

## B. Verwerkingsverantwoordelijke

6. In het proces dat leidt tot de afgifte van een identiteitskaart is niet eenduidig bepaald wie de verwerkingsverantwoordelijke(n) is(zijn):

- Artikel 6, § 1, eerste lid, van de wet van 19 juli 1991, bepaalt dat de gemeente een identiteitskaart of vreemdelingenkaart geeft als bewijs van inschrijving in de bevolkingsregisters.
- Krachtens artikel 6, § 5, eerste lid, stelt de federale overheid de nodige apparatuur voor de elektronische kaart ter beschikking van de gemeente.
- Artikel 3 van het koninklijk besluit specificeert dat de minister van Binnenlandse Zaken de identiteitskaart aan de gemeentebesturen levert en dat hij het model van het basisdocument van de identiteitskaart vaststelt.
- In de *Algemene onderrichtingen betreffende de elektronische identiteitskaarten van de Belg*<sup>2</sup> van de FOD Binnenlandse Zaken vinden we het volgende terug: *"Het Rijksregister van de natuurlijke personen is de draaischijf van het systeem. Deze dienst verzekert de coördinatie tussen de aanvrager van de elektronische identiteitskaart in de gemeente en het contact met de producent, de personalisator en de initialisator van de kaart. Alle fasen van het productieproces worden aan het Rijksregister gemeld. Het RR vraagt ook de certificaten van de authenticatie en de elektronische handtekening aan de certificatedienst. De initialisator bereidt de veiligheidssleutels voor. Het RR controleert of het toegekende sleutelpaar uniek is: de openbare sleutel wordt gecontroleerd, de privé sleutel is niet gekend. Het RR bereidt de gegevens voor om een certificaat voor het gecontroleerde sleutelpaar aan te vragen: het RR geeft het certificaatnummer en vraagt een erkende certificatedienst om een certificaat af te leveren. De erkenning van de certificatedienst voldoet aan de voorwaarden van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatediensten en aan de Europese eisen op dit domein. Het Rijksregister van de natuurlijke personen houdt een centraal bestand van de identiteitskaarten bij dat "Register van de identiteitskaarten" wordt genoemd".*

7. In de DPIA die de Autoriteit mocht ontvangen, wordt op blz. 4 gepreciseerd dat de FOD Binnenlandse Zaken verwerkingsverantwoordelijke is, worden er een aantal verwerkers geïdentificeerd en wordt er gewag gemaakt van partners. Inzake gegevensverwerking kent de AVG geen partners. Zij kent alleen verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken, verwerkers en derden (artikel 4.7), 8) en 10) en artikel 26 AVG).

---

<sup>2</sup> [https://www.ibz.rrn.fgov.be/fileadmin/user\\_upload/nl/kaarten/eid/onderrichtingen/AO-eID-25052018.pdf](https://www.ibz.rrn.fgov.be/fileadmin/user_upload/nl/kaarten/eid/onderrichtingen/AO-eID-25052018.pdf) (gecoördineerde versie van 2 mei 2017, laatste bijwerking 25 mei 2018).

8. De afgifte van identiteitskaarten vereist een massale gegevensverwerking die gepaard gaat met een hele reeks van verwerkingsprocessen en de betrokkenheid van een grote waaier actoren (FOD Binnenlandse Zaken, gemeenten, producent, ICT-firma's, ...). Het is de hoogste tijd dat in de regelgeving wordt geïdentificeerd wie (gezamenlijke)-verantwoordelijk(en) /verwerker is (zijn) voor wat zodat het voor iedereen duidelijk is op wie de verantwoordelijkheid rust om ervoor te zorgen dat zowel de bepalingen van de AVG als de specifieke wettelijke bepalingen ter zake worden gerespecteerd. Al naargelang het geval zal dan artikel 24, dan wel 26 of 28 AVG moeten in acht worden genomen.

### **C. Doel van de verwerking**

9. Uit de lectuur van artikel 6 van de wet van 19 juli 1991 en artikel 3 van het koninklijk besluit kan, zonder dat het er met zoveel woorden instaat, worden afgeleid dat de identiteitskaart wordt verstrekt en bijgevolg daartoe persoonsgegevens worden verwerkt, voor volgende doeleinden:

- het bewijs leveren dat iemand is ingeschreven in de bevolkingsregisters (artikel 6, § 1, eerste lid, van de wet van 19 juli 1991);
- het vaststellen van de identiteit van een persoon (artikel 1 en artikel 3, § 1, eerste lid, van het koninklijk besluit);
- toelaten iemand op afstand elektronisch te identificeren en authenticeren.

10. Deze doeleinden zijn welbepaald, uitdrukkelijk omschreven en gerechtvaardigd (artikel 5.1.b) AVG).

11. De Autoriteit stelt vast dat de wetgever zijn goedkeuring hechtte aan de opslag van de vingerafdrukken omdat de bevoegde minister hamerde op de noodzaak om de strijd tegen identiteitsfraude te versterken (wat kan worden bestempeld als zijnde een kennelijk verenigbaar doeleinde met deze vermeld in punt 9). In de DPIA, die door de aanvrager werd bezorgd, wordt echter het volgende vermeld: "*La justification de la finalité concernant la vérification de l'identité peut être améliorée, la justification liée à la lutte contre la fraude à l'identité ne tient pas*". In de DPIA wordt dus het geweer van schouder veranderd. Daarin wordt thans benadrukt dat de identiteitskaart een reisdocument is en bijgevolg moet voldoen aan de internationale vereisten van een reisdocument, een argument dat zijdelings werd aangeraakt tijdens de parlementaire discussie.

12. De identiteitskaart werd niet geconcipeerd als een reisdocument zoals uit de doeleinden blijkt. Dat een aantal landen de Belgische identiteitskaart aanvaarden als een reisdocument, is het gevolg van een akkoord met de landen voor wie de identiteitskaart zoals ze momenteel bestaat een voldoende

betrouwbaar alternatief is voor een paspoort en bijgevolg niet alle toeters en bellen van een paspoort moet hebben.

13. Trouwens, een niet onbelangrijk percentage van de Belgen reist niet. Ten overstaan van hen is het opslaan van de vingerafdrukken op de identiteitskaart in het licht van artikel 5.1.c) AVG dan ook een manifest disproportionele maatregel. En voor de Belgen die reizen: waarom laat men hen niet de keuze tussen een identiteitskaart met vingerafdrukken dan wel een paspoort?

14. De geldigheidsduur van de identiteitskaart bedraagt 10 jaar. Volgens de bijkomende informatie zullen de vingerafdrukken slechts aangebracht worden n.a.v. de vernieuwing van de identiteitskaarten. Dit wil dus zeggen dat gedurende 10 jaar 2 soorten identiteitskaarten in omloop zullen zijn. Er kunnen dus vraagtekens geplaatst worden bij het nut van de operatie die 10 jaar in beslag zal nemen en dus ook bij het nut om de vingerafdrukken op de identiteitskaart aan te brengen. Dit lijkt er eens te meer op te wijzen dat de identiteitsfraude niet zo'n groot en ernstig probleem is als men liet uitschijnen. De DPIA bevestigt dit trouwens.

## **D. Gegevens en proportionaliteit**

15. De gegevens die op de identiteitskaart worden vermeld en die dus ook met het oog daarop worden ingezameld, worden vastgesteld door artikel 6 van de wet van 19 juli 1991, bepaling die reeds het voorwerp uitmaakte van adviezen van de Autoriteit<sup>3</sup>, waar hier volledigheidshalve naar wordt verwezen.

### ***D.1. Elektronisch chip (vervangt elektronische microprocessorchip)***

16. Voor nadere commentaar over de elektronische chip wordt verwezen naar het technisch analyseverslag in bijlage.

17. Artikel 6, § 4, tweede lid, van de wet van 19 juli 1991 bepaalt: "*Het Rijksregisternummer en de foto van de houder mogen enkel gebruikt worden indien hiertoe gemachtigd is door of krachtens een wet, decreet of een ordonnantie (...)*". Een mooi principe dat in de praktijk niets voorstelt. De foto, die ook verplicht digitaal wordt opgeslagen op de chip, wordt op geen enkele manier beschermd. De overheid verstrekt de burger dus een instrument waardoor dit gegeven niet specifiek wordt beschermd. De burger heeft geen enkele controle over de data die al dan niet elektronisch mogen worden gelezen. In de memorie van toelichting werd dit bezwaar als volgt ontzenuwd<sup>4</sup>:

---

<sup>3</sup> Advies nr. 19/2018 van 28 februari 2018 van de Commissie voor de bescherming van de persoonlijke levenssfeer en advies nr. 106/2018 van 17 oktober 2018 van de Autoriteit.

<sup>4</sup> Kamer, doc 54 – 3256/001 – blz. 39.

*"De Commissie beveelt eveneens aan dat de wet de betrokken verantwoordelijken voor de verwerking zou verplichten om de nodige middelen ter beschikking te stellen van de betrokken persoon om te beslissen welke gegevens hij/zij aan de hand van zijn/haar kaart meedeelt (zie punt 75). Deze mogelijkheid kan echter niet overwogen worden, omdat dat te complex is voor de burger".*

18. Het huidige concept van de elektronische identiteitskaart dateert ondertussen van 15 jaar geleden. Vraag is of ondertussen ernstig werd onderzocht of het, rekening houdend met de huidige stand van de technologie, mogelijk is om de burger een kaart af te leveren die hem toelaat zijn gegevens beter te beschermen. Momenteel kan de identiteitskaart moeilijk bestempeld worden als een voorbeeld van privacy by design.

19. De burger staat met lege handen. Hij is zonder meer verplicht om uit te gaan van de goede trouw van iedereen die zijn identiteitskaart leest. Wanneer hij instemt met de lectuur van zijn kaart heeft hij geen enkele garantie dat de informatie die wordt gelezen, waaronder de foto, ook niet wordt opgeslagen. Wanneer zijn kaart wordt gestolen of hij zijn kaart verliest wordt identiteitsdiefstal wel erg makkelijk.

## ***D.2. Tweedimensionale barcode***

20. Het ontwerp – artikel 3, 1<sup>o</sup> - voert echter een reglementaire nieuwigheid in. Er wordt namelijk uitdrukkelijk bepaald dat de identiteitskaart een tweedimensionale barcode zal bevatten. Uit de bijkomende informatie verstrekt door de aanvrager op 15/03/2019 blijkt dat de artikel 6 van de wet van 19 juli 1991 in de praktijk aanleiding heeft gegeven tot de opname van 2 systemen van elektronisch leesbare persoonsgegevens op de identiteitskaart, namelijk via:

- een elektronische microprocessorchip, die alle in de wet opgesomde elektronisch leesbare informatie bevat
- een barcode waarvan niet duidelijk is welke elektronisch leesbare informatie ze bevat.

21. In het koninklijk besluit (uitvoeringsbesluit) was alleen sprake van een elektronische microprocessorchip. De Autoriteit stelt vast dat de voorgenomen wijziging ertoe strekt een reeds van toepassing zijnde praktijk te legaliseren. De actuele identiteitskaarten bevatten reeds dergelijke barcode, zonder dat dit in de regelgeving gespecificeerd werd en zonder dat werd verduidelijkt welke informatie deze barcode bevat. De aanvrager meldde dat achter de barcode de volgende informatie schuilgaat: het Rijksregisternummer, het kaartnummer, de geldigheidsduur en de geboortedatum. Met

het oog op duidelijkheid en transparantie moet dit op zijn minst in het koninklijk besluit worden gepreciseerd.

22. Het doeleinde met het oog waarop een barcode wordt voorzien is volgens de bijkomende informatie, verstrekt door aanvrager, tweevoudig:

- het controleren van de gegevens die op de kaart zijn gedrukt (hieruit leidt de Autoriteit af dat het de bedoeling is om eventuele manipulatie van de gedrukte gegevens op de kaart te detecteren);
- de snelle toegang tot een beperkt aantal gegevens wanneer een lectuur met een kaartlezer niet mogelijk is.

23. De vraag is of het aanbrengen van een barcode een effectief middel is om het eerste doeleinde te bereiken: als men erin slaagt om de opdruk van de gegevens op de identiteitskaart te manipuleren, belet ook niets dat aan deze barcode wordt gesleuteld.

24. Men heeft geen barcode nodig om snel toegang te hebben tot bepaalde informatie vermeld op de identiteitskaart. De informatie die achter de barcode schuilgaat, staat op de kaart gedrukt en is dus *de visu* onmiddellijk (= snel) raadpleegbaar. In de mate dat het de bedoeling is om bijvoorbeeld de leeftijd te controleren wanneer men iets uit een automaat wenst te verkrijgen (sigaretten, alcohol), dan volstaat het dat de leeftijd onder de vorm van een barcode wordt vermeld.

25. De Autoriteit kan zich niet van de indruk ontdoen dat de bedoeling van de barcode erin bestaat om snel elektronisch informatie te verzamelen m.b.t. personen waarbij niet duidelijk is voor wie deze faciliteit is bedoeld, noch waarom zij deze informatie verzamelen. Indien dit het geval is moet dit nader worden gepreciseerd.

26. Een snelle toegang tot een beperkte set van gegevens is ook vanuit commercieel oogpunt interessant. Een nietsvermoedende burger die zijn identiteitskaart toont, bijvoorbeeld om te bewijzen dat hij voldoet aan de leeftijdsvereiste om een bepaald goed te krijgen, zal er geen graten in zien dat de winkelier zijn identiteitskaart even onder een barcodescanner houdt, omdat hij niet beseft dat daardoor zijn persoonsgegevens worden gelezen. Hij heeft geen garantie dat n.a.v. de scanning van de barcode de gegevens die erop staan niet worden opgeslagen. Aan de hand van de gegevens die also kunnen gecapteerd worden, kan men op internet al behoorlijk ver komen om zich voor te doen als iemand die men niet is: men heeft het Rijksregisternummer, het nummer van de identiteitskaart en de geboortedatum, zijnde gegevens die niet zelden door websites worden gebruikt om iemand te identificeren.



27. Het risico dat de barcode identiteitsfraude op het internet bevordert, is dus reëel en staat dus haaks op wat men met de operatie wenst te bereiken. In de DPIA die werd bezorgd, werd geen enkele aandacht besteed aan dit aspect, niettegenstaande de potentieel schadelijke gevolgen voor de rechten en vrijheden van de betrokkene.

### ***D.3. Ad hoc sensor***

28. Het ontwerp vult artikel 3 van het koninklijk besluit aan met een nieuwe paragraaf 5. In het tweede lid van deze paragraaf wordt gepreciseerd: "*De vingerafdrukken worden op initiatief van de ambtenaar van de burgerlijke stand of van zijn afgevaardigde door middel van een ad hoc sensor gedigitaliseerd. Dit digitale beeld wordt vervolgens door middel van de diensten van het Rijksregister overgezonden aan de producent van de identiteitskaart om erin te worden geïntegreerd*".

29. Voor wat deze problematiek betreft wordt verwezen naar het technisch analyseverslag in bijlage.

### ***D.4. Niet vermelden van de wettelijk voorgeschreven gegevens***

30. De wet bepaalt dat de identiteitskaart de handtekening van de houder bevat. Artikel 3, § 3, van het koninklijk besluit stelt dat indien de houder niet kan tekenen, ingevolge analfabetisme, handicap of ziekte, de handtekening vervangen wordt door de vermelding "vrijgesteld". Momenteel wordt dit bewijs geleverd (behoudens wanneer het duidelijk zichtbaar is) door middel van een "recent attest". Ingevolge artikel 3, 6°, van het ontwerp wordt "recent attest" vervangen door "**medisch attest** van minder dan een maand".

31. Er zullen bijgevolg ontegensprekelijk bijzondere categorieën van persoonsgegevens in de zin van artikel 9 AVG worden verwerkt, zonder dat men enig zicht op heeft op een aantal essentiële elementen van de verwerking zoals:

- wie de verwerkingsverantwoordelijke is: is het de ambtenaar van de burgerlijke stand (en bij uitbreiding de gemeente ) die op basis van het attest de beslissing neemt? Of trancheert de Minister van Binnenlandse Zaken/ de FOD Binnenlandse Zaken?;
- wordt het attest op de gemeente bewaard of wordt het bezorgd aan de Minister van Binnenlandse Zaken/ de FOD Binnenlandse Zaken om daar te worden bewaard? ;
- hoelang de informatie wordt bewaard en waarom?

32. Voor deze verwerking moet door de aanvrager een verwerkingsgrond op basis van artikel 9.2 AVG worden geïdentificeerd.

33. Artikel 6, § 2, derde lid, van de wet van 19 juli 1991 bepaalt dat de vingerafdrukken van de wijsvinger van de linker- en van de rechterhand wordt opgenomen of ingeval van ongeschiktheid van een andere vinger van elke hand, waarbij de Koning nadere regels bepaalt.

34. Zoals reeds werd aangestipt vult het ontwerp artikel 3 van het koninklijk besluit aan met een nieuwe paragraaf 5. De leden 4 tot 7 van deze paragraaf regelen de gevallen waarin er een identiteitskaart of vreemdelingenkaart wordt uitgereikt zonder vingerafdrukken, dit terwijl de wet niet voorziet dat er identiteitskaarten zonder vingerafdrukken kunnen worden uitgereikt en de delegatie aan de Koning dit evenmin voorziet.

35. Gelet op het feit dat de Autoriteit geen voorstander is van het opnemen van vingerafdrukken op de identiteitskaart, is het voorzien van situaties waarin geen vingerafdrukken worden opgenomen *an sich* vanuit perspectief van gegevensverwerking dus niet problematisch. Dit neemt niet weg dat het door het ontwerp uitgewerkte regime van "**vingerafdrukloze**" identiteitskaarten toch aanleiding geeft tot een aantal bedenkingen.

36. Er zal een identiteitskaart zonder vingerafdrukken worden uitgereikt wanneer de houder:

- permanent of gedurende meer dan 3 maanden geen vingerafdrukken kan geven omwille van een fysieke handicap of ziekte. Het bewijs wordt geleverd door een medisch attest, behalve wanneer het duidelijk is dat de betrokkene niet in staat is om zijn vingerafdrukken te geven omwille van een fysieke handicap of een duidelijk zichtbare ziekte;
- door een lichamelijke bijzonderheid geen vingerafdrukken kan geven die goed genoeg zijn om vastgelegd te worden. Het is de gemeenteburgemeester die deze onmogelijkheid beoordeelt;
- zich permanent of gedurende meer dan 3 maanden niet kan verplaatsen om zijn vingerafdrukken te geven. Het bewijs wordt geleverd door een medisch attest;
- zich onmogelijk kan verplaatsen gedurende meer dan 3 maanden om zijn vingerafdrukken te geven ingevolge een gerechtelijke beslissing. Het bewijs wordt geleverd door middel van een kopie van deze gerechtelijke beslissing.

37. Als men kijkt naar de cijfers die in het parlement werden geciteerd n.a.v. de behandeling van het wetsontwerp waardoor de vingerafdrukken op de identiteitskaart werden ingevoerd, dan kan men niet anders dan vaststellen dat het aantal gevallen van identiteitsfraude met de identiteitskaart en "lookalike" fraude zeer gering is (de bevoegde minister verschaftte aan het parlement volgende cijfers: vastgestelde identiteitsfraude met identiteitskaart in 2018: 566; "lookalike" fraude: 159 gevallen

tijdens het eerste half jaar van 2018<sup>5</sup> - ter verduidelijking, er zijn ca 11 miljoen identiteitskaarten en vreemdelinge kaarten in omloop).

38. De Autoriteit is er zich wel van bewust dat identiteitsfraude meestal slechts een onderdeel is van een ruimer crimineel opzet. De hierboven geformuleerde uitzonderingen bieden echter interessante perspectieven voor personen die de intentie hebben om fraude te plegen en daartoe in het bezit wensen te komen van een "vingerafdrukloze" identiteitskaart.

39. Het bewijs van de onmogelijkheid om vingerafdrukken te verstrekken kan in 2 gevallen geleverd worden aan de hand van een **medisch attest**. Er worden regelmatig blanco medische attesten gestolen, die worden verkocht en die vervolgens naar goeddunken kunnen worden ingevuld. Zij kunnen ook vrij gemakkelijk worden nagemaakt. Hoe gaat de gemeentelijke beambte aan wie een dergelijk attest wordt voorgelegd kunnen uitmaken of het om een bonafide attest betreft?

40. Volledigheidshalve verwijst de Autoriteit voor wat de problematiek van het medisch attest betreft, naar de opmerkingen geformuleerd in punt 31.

41. De **gemeenteambtenaar** is bevoegd om de lichamelijke bijzonderheid te **beoordelen** die belet om vingerafdrukken te geven die goed genoeg zijn om vastgelegd te worden. Deze omschrijving laat een ruime appreciatiebevoegdheid aan de gemeenteambtenaar en dus de mogelijkheid voor personen met malafide bedoelingen om daarop in te spelen door bijvoorbeeld een ambtenaar te bedreigen. Het is daarenboven niet duidelijk of dergelijke beslissing wordt geregistreerd en zo ja, waar? Evenmin is duidelijk of die beslissing wordt gedocumenteerd en zo ja waar en hoe lang die informatie wordt bewaard? In de gegeven omstandigheden kan de Autoriteit niet beoordelen of dit leidt tot een bijkomende verwerking van persoonsgegevens en wie daarvoor als verwerkingsverantwoordelijke moet worden gekwalificeerd. Dit moet dus nader worden gepreciseerd.

42. Iemand die ingevolge een gerechtelijke beslissing niet in de mogelijkheid is om zich gedurende een periode van meer dan 3 maanden te verplaatsen om zijn vingerafdrukken te geven, wordt eveneens vrijgesteld. Volgens de bijkomende informatie ontvangen op 15/03/2019 worden hierdoor onder meer gevangenen geviseerd. Concreet betekent dit dus iemand die veroordeeld is tot een gevangenisstraf van 5 jaar en wiens identiteitskaart in de loop van het 4<sup>o</sup> jaar van zijn gevangenisstraf aan vernieuwing toe is, een identiteitskaart zonder vingerafdrukken zal krijgen terwijl burgers die nooit enige veroordeling opliepen wel hun vingerafdrukken moeten prijsgeven.

---

<sup>5</sup> Kamer, doc 54 – 3256/003, blz. 31-34.

43. Er zullen dus identiteitskaarten zonder vingerafdrukken in omloop komen. De Autoriteit stelt voor dat in het koninklijk besluit een analoge regeling wordt voorzien als deze bij afwezigheid van een handtekening op de identiteitskaart, namelijk dat de vingerafdrukken vervangen worden door de vermelding "vrijgesteld". Het is aangewezen om dergelijke beveiligde vermelding aan te brengen op de chip waarop normaal de vingerafdrukken moeten staan.

## **E. Betrokkenen**

44. Zij worden bepaald in artikel 6, eerste lid van de wet van 19 juli 1991. Het betreft Belgen en vreemdelingen die ingeschreven zijn in de bevolkingsregisters.

## **F. Entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt**

45. Voor wat de vingerafdrukken betreft bepaalt artikel 6, § 2, zesde lid van de wet van 19 juli 1991 de entiteiten die de vingerafdrukken mogen lezen evenals de doeleinden waarvoor ze dit mogen. In een aantal gevallen wordt daarbij gewag gemaakt van "fraudebestrijding", versta bestrijding van identiteitsfraude.

46. De wet is duidelijk: de geviseerde entiteiten mogen alleen maar "lezen". Dit betekent dat de opslag van de vingerafdrukken zo moet worden geconcipieerd dat ze niet elektronisch kunnen worden gekopieerd, noch uitgelezen door niet specifiek daarvoor bestemde apparatuur. Uit de documenten die door de aanvrager werden verschaft, blijkt dit niet.

47. De Autoriteit stelt vast dat het louter lezen en dus bekijken van de vingerafdrukken die op de kaart staan, niet zal volstaan om na te gaan of de vingerafdrukken van de persoon die zich aanbiedt met een kaart, dezelfde zijn als diegene die op de kaart staan. Het vereist dat de betrokkene zijn vingers in een "leestoestel" plaatst en dat er vervolgens een vergelijking wordt gemaakt tussen het beeld op de kaart en het beeld op het leestoestel. Er moet dus hoe dan ook wel wat meer worden gedaan dan juist de vingerafdrukken "lezen".

## **G. Opslagperiode**

48. Een aantal van de gegevens die op de identiteitskaart zijn vermeld, worden opgeslagen in het Register van identiteitskaarten, waarvan de bewaartermijn wettelijk geregeld is. De vingerafdrukken worden niet in dit register opgenomen. De opslagduur ervan - buiten de identiteitskaart - is wettelijk vastgesteld op 3 maanden, termijn binnen dewelke de identiteitskaart normaal moet kunnen worden aangemaakt (artikel 6, § 2, wet van 19 juli 1991). Het is de verwerkingsverantwoordelijke die voor de

naleving hiervan instaat. Wie is de verwerkingsverantwoordelijke die ervoor moet zorgen dat deze bepaling wordt nageleefd? Noch de wet noch het ontwerp verschaffen daarover duidelijkheid (zie ook punt 8).

49. De FOD Binnenlandse Zaken staat in voor de centrale opslag van de vingerafdrukken gedurende een periode van 3 maanden. Uit de DPIA (blz. 7) leidt de Autoriteit af dat de vingerafdrukken samen met alle andere gegevens die op de identiteitskaart worden vermeld, ook gedurende 1 maand bij de producent van de kaarten worden opgeslagen. Dit betekent dat er op 2 plaatsen een groot aantal gegevens, bijzondere gegevens (artikel 9 AVG), worden gestockeerd waardoor het risico een inbreuk in verband met persoonsgegevens substantieel toeneemt. Op bladzijde 8 van de DPIA leest men dat "*Il est prévu d'organiser, à court terme, un contrôle d'effectivité des effacements*". Als tot op heden geen controle geschiedde op het wissen van de gegevens die de verwerkers met het oog op de aanmaak van de identiteitskaarten ontvingen, dan is dat niet bepaald vertrouwenwekkend.

50. Vermits de geldigheidsduur van de identiteitskaart 10 jaar bedraagt, worden de vingerafdrukken gedurende 10 jaar op die drager bewaard. Gedurende die periode heeft de titularis van de kaart, binnen het reglementair vastgelegde kader, de controle over de informatie die de identiteitskaart bevat. Wanneer de geldigheidsduur van de kaart ten einde loopt zal hij deze, naar aanleiding van de afgifte van zijn nieuwe identiteitskaart, afgeven aan een bevoegde ambtenaar van de gemeente.

51. Momenteel is niet duidelijk wat er vervolgens met de ingeleverde identiteitskaart gebeurt. Wordt die door de gemeente vernietigd? Zo ja wanneer wordt ze vernietigd en hoe? Wordt de vernietiging uitbesteed aan derden? Worden die ingeleverde identiteitskaarten centraal verzameld en vervolgens vernietigd? Zo ja door wie? Wanneer worden ze vernietigd en hoe?

52. Dit aspect moet duidelijk geregeld worden. De Autoriteit is van oordeel dat, gelet op het zeer intrusief karakter van de vingerafdrukken op de identiteitskaart, mag worden geëist dat de ingeleverde identiteitskaart in aanwezigheid van de houder ervan wordt vernietigd.

## **H. Andere opmerkingen**

### ***H.1. Moment van opname op de vingerafdrukken op de identiteitskaart***

53. Het eerste lid van de nieuwe § 5 van artikel 3 stelt dat de minister bevoegd voor Binnenlandse Zaken de datum bepaalt waarop identiteitskaarten en vreemdelingenkaarten de vingerafdrukken

moeten bevatten. De minister bevoegd voor Buitenlandse Zaken doet hetzelfde voor de in artikel 39 *Consulair Wetboek* bedoelde identiteitskaarten voor Belgen in het buitenland.

54. Overeenkomstig artikel 39 *Consulair Wetboek* draagt de door de consulaire post afgegeven identiteitskaart "*identieke kenmerken*" als de identiteitskaart die in België aan een Belg wordt afgeleverd<sup>6</sup>. Noch het *Consulair Wetboek*, noch het koninklijk besluit van 19 april 2014 *aangaande identiteitskaarten afgegeven door de consulaire beroepsposten*, bevat momenteel geen enkele van de krachtens artikel 6.3 AVG vereiste preciseringen. Dit wetboek/besluit zal dus moeten worden aangepast met het oog op de afgifte van identiteitskaarten die vingerafdrukken bevatten.

55. De Autoriteit benadrukt de noodzaak om voorafgaandelijk een grondige gegevensbeschermingseffectbeoordeling uit te voeren (artikel 35.3.b) AVG). Het gaat om de grootschalige verzameling van gevoelige gegevens met een hoog risico voor de rechten en vrijheden van de betrokkenen, door actoren verspreid over de hele wereld, en die vervolgens worden overgemaakt aan o.a. een verwerker met het oog op de fabricatie van de identiteitskaart.

## ***H.2. Artikel 4 van het ontwerp (voegt een artikel 3/1 in)***

56. Een burger zal *de facto* zijn nieuwe kaart maar ontvangen nadat de gemeenteambtenaar zowel de foto als de vingerafdrukken op de kaart heeft vergeleken met het gezicht en de vingerafdrukken van de persoon die zich aanbiedt.

57. Gelet op het feit dat er identiteitskaarten zonder vingerafdrukken worden uitgereikt, is het aangewezen om voor wat de vingerafdrukken betreft misschien te verduidelijken "voor zover er vingerafdrukken op de kaart werden aangebracht".

## ***H.3. Artikel 6 van het ontwerp (vervangt het huidige artikel 6 van het koninklijk besluit)***

58. Artikel 6 *ter* van de wet van 19 juli 1991 bepaalt dat ingeval van verlies, diefstal of vernieling aangifte wordt gedaan bij het gemeentebestuur, de politie of de helpdesk van het Rijksregister voor wat de identiteitskaart van een Belg betreft en bij de politie voor wat de vreemdelingenkaart betreft. Naar aanleiding van de aangifte wordt een attest uitgereikt. Artikel 6 van het ontwerp werkt deze bepaling verder uit.

---

<sup>6</sup> Dit wordt trouwens ook expliciet benadrukt door artikel 6, § 1, derde lid, van de wet van 19 juli 1991.

59. Voor wat de identiteitskaart betreft:

- bij het gemeentebestuur van zijn woonplaats tijdens de kantooruren (§ 1, eerste lid). Het bestuur levert een attest van verlies, diefstal of vernietiging af en geeft de opdracht aan de certificatieverlener om de elektronische functies van de kaart in te trekken zodat deze definitief buiten werking worden gesteld door de identiteitskaart te annuleren;
- bij de Helpdesk van het Rijksregister die de elektronische functies intrekt. De betrokkene moet dan naderhand nog wel bij de gemeente langs gaan met het oog op de verstrekking van een attest en de annulatie van de identiteitskaart;
- bij de politie buiten de kantooruren of indien het gemeentebestuur niet bereikbaar is. De politie levert het attest af en stuurt een kopie ervan naar de Helpdesk van het Rijksregister met het oog op de intrekking van de elektronische functies en deze laatste verwittigt vervolgens de gemeente opdat deze de kaart zou annuleren.

60. Voor wat de vreemdelinge kaart betreft gebeurt de aangifte altijd bij de politie. De politie levert het attest af en stuurt een kopie ervan naar de Helpdesk van het Rijksregister met het oog op de intrekking van de elektronische functies en deze laatste verwittigt vervolgens de gemeente opdat deze de kaart zou annuleren.

61. Voor een goed begrip: wanneer in de tekst gesproken wordt van de elektronische functies van de kaart die worden ingetrokken, betekent dit concreet het buiten werking stellen van de certificaten. De elektronisch leesbare informatie op een verloren of gestolen kaart, zal elektronisch leesbaar blijven.

62. De Helpdesk van het Rijksregister ontvangt vanwege de politie een kopie van het attest van verlies, diefstal of vernietiging van de kaart<sup>7</sup> zodat eerstgenoemde laatste de elektronische functies kan deactiveren. Gelet op het feit dat er geen tijd mag worden verloren bij het intrekken van de certificaten, veronderstelt de Autoriteit dat een kopie van dit attest op elektronische wijze aan de Helpdesk wordt bezorgd. Artikelen 5.1.f), 24.1 en 32 van de AVG vermelden uitdrukkelijk de verplichting voor de verwerkingsverantwoordelijke om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's. Bij gebrek aan enige informatie omtrent de wijze waarop deze mededeling geschiedt, drukt de Autoriteit de hoop uit dat de toezending

---

<sup>7</sup> In het voorgestelde nieuwe artikel 6, § 4, van het koninklijk besluit wordt gewag gemaakt van een model van attest. Volgens bijkomende informatie ontvangen op 20/03/2019 is het een verwijzing naar het model dat als bijlage aan het huidige koninklijk besluit is toegevoegd.

van de kopieën van de attesten via een beveiligd kanaal geschiedt en niet per gewone e-mail. Het gebruik van dit laatste middel is in het licht van de hiervoor vermelde elementen immers problematisch. De kopie van het attest is voor de Helpdesk van het Rijksregister het equivalent van de opdracht om de certificaten te deactiveren. In geval van discussie of betwisting beschikt de Helpdesk ook over een bewijsstuk. Er wordt nergens bepaald wat de Helpdesk van het Rijksregister met deze kopieën doet en hoelang deze worden bewaard. In het licht van artikel 5.1.e) AVG moet dit nader in het besluit worden gepreciseerd.

63. Het voorgestelde nieuwe artikel 6, § 5 van het koninklijk besluit, voorziet dat een identiteitskaart of vreemdelingenkaart die teruggevonden wordt, moet worden ingeleverd bij het gemeentebestuur ongeacht of de houder reeds een vernieuwde kaart ontving of niet. Volgens het huidige koninklijk besluit moet een teruggevonden kaart alleen worden ingeleverd wanneer ze wordt gevonden nadat de kaart van de houder werd vernieuwd.

64. Er wordt niet gepreciseerd wat er met de ingeleverde kaart gebeurt. Wordt een ontvangstbewijs verstrekt aan diegene die de kaart inlevert? Wordt ze, na reactivering van de certificaten, aan de houder terugbezorgd als hij nog geen nieuwe kaart ontving? Wordt de kaart vernietigd door de gemeente en hoe gebeurt dit? Worden de kaarten bezorgd aan het Rijksregister dat instaat voor de vernietiging? Wordt de ambtshalve vernietiging gedocumenteerd en geregistreerd? Dit moet nader worden gepreciseerd in het besluit (zie ook punten 51-52).

## **J. Technische synthese**

65. Op basis van de DPIA die de Autoriteit mocht ontvangen, werd een technische analyse verricht die heel wat vragen oproept, zowel op het vlak van beveiliging als de integriteit van het proces (zie vertrouwelijke bijlage).

66. De Autoriteit formuleert evenwel het volgende voorbehoud.

67. Betreffende de informatie in het ontvangen document over de gebruikte chiptechnologie, wordt het gebruik vermeld van een ROM-geheugen (Read Only Memory). Welnu, bij dit type technologie wordt de inhoud van het geheugen opgeslagen bij de fabricatie. Er is dus twijfel bij het gebruik van een ROM-geheugen op het niveau van de RFID chip. Wij denken dat het veeleer gaat om een EEPROM (Electrically Erasable Programmable Read Only Memory) die dus kunnen gewist worden en elektrisch geherprogrammeerd.



68. In de ontvangen informatie wordt gewag gemaakt van de voorschriften en aanbevelingen van de ICAO in het raam van het MRTD (Machine Readable Travel Document) terwijl het in dit geval gaat om eMRTD's (electronic Machine Readable Travel Documents). Er wordt in de normen wel degelijk verwezen naar Doc. 9303 Zevende Editie, 2015 Deel 1, Deel 3 en deel 5 van de ICAO, doch er is geen enkel spoor van Deel 11 van Doc. 9303 dat handelt over de veiligheidsmechanismen van de MRTD's en meer in het bijzonder over de te overwegen bijkomende maatregelen in het raam van de eMRTD's. Dit Deel 11 levert immers specificaties die de staten en leveranciers toelaten om te voorzien in cryptografische beveiligingsfuncties voor contactloos machineleesbare elektronische reisdocumenten ("eMRTD's") met geïntegreerde schakeling (elektronische chip). De cryptografische protocollen worden gespecificeerd om:

- aanvallen via "skimming" van de gegevens opgeslagen op de RFID chip te beletten
- aanvallen via "eavesdropping" (onwettig onderscheppen van communicaties) tussen de chip en de lezer te beletten
- de authenticatie te verzekeren van de in de chip contactloos opgeslagen gegevens op basis van de openbare sleutelinfrastructuur (PKI) beschreven in Deel 12 van Doc. 9303 (ook niet vermeld)
- de contactloze authenticatie van de chip verzekeren.

Er dient te worden opgemerkt dat de huidige editie van Doc. 9303 in geen enkele bijkomende toegangscontrole voorziet voor gevoelige gegevens (t.t.z. secundaire biometrische elementen), met andere woorden de foto en vingerafdrukken, maar dat het toepassen van nationale mechanismen om deze gegevens te beschermen toegelaten is. Het is de bedoeling om hiervoor een interoperabele specificatie op te nemen in toekomstige versies van Doc. 9330. Er wordt geen informatie verstrekt over de mechanismen die België van plan is in te voeren om de toegang tot deze gegevens te beschermen. De tabel toont de verschillende beschikbare opties met, in het blauw, de maatregelen die verondersteld worden te zijn weerhouden voor de nieuwe eID.

69. De beschermende maatregelen beletten niet de exacte kopie of vervanging van de chip. Dit vormt een integriteitsprobleem voor het document en garandeert dus niet de authenticiteit.

70. De maatregelen die de nieuwe risico's, namelijk op skimming en interceptie van communicatie, die worden veroorzaakt door het gebruik van contactloze chips (RFID) verminderen, berusten op cryptografie. Welnu, de zwakke punten van cryptografische maatregelen roepen twee vragen op: Wat doet men indien de sleutels worden gekraakt? Mogelijk scenario, hetzij ingeval van diefstal van de sleutels, of bij toename van de rekenkracht ingevolge de evolutie van technologieën. Waaruit zullen de technologische mogelijkheden binnen 10 jaar bestaan? Zullen de gebruikte algoritmen en sleutellengte, de vandaag geplande certificaten, binnen 10 jaar nog steeds betrouwbaar

zijn gelet op de snelheid van de technologische evolutie, voornamelijk de rekenkracht die we van kwantumcomputers kunnen verwachten?

**OM DEZE REDENEN,  
de Autoriteit**

↳ is van oordeel dat volgende aanpassingen zich opdringen:

- preciseren van de (gezamenlijke) verantwoordelijken/verwerkers (punten 7 en 8);
- controle van de burger op zijn gegevens verhogen door gepaste technische maatregelen (punten 17-19);
- preciseren welke informatie achter de barcode schuilgaat (punt 21);
- nut en veiligheid van de barcode in zijn huidige vorm herbekijken (punten 25-27);
- voor wat de medische attesten betreft die verstrekt worden met het oog op vrijstelling van handtekening en vingerafdrukken preciseren op welke rechtsgrond dat wordt gesteund, wie de verwerkingsverantwoordelijke is, hoe lang ze worden bewaard (punten 31 en 40);
- maatregelen voorzien om misbruik van de vrijstellingsregeling te voorkomen (punten 39 en 41);
- preciseren m.b.t. beslissingen waarbij vrijstelling van vingerafdrukken wordt verleend wie verwerkingsverantwoordelijke is, hoe lang ze worden bewaard (punt 41);
- vermelding "vrijstelling" aanbrengen op de chip van een identiteitskaart/vreemdelingenkaart zonder vingerafdrukken (punt 43);
- de vernietiging van de identiteitskaart/vreemdelingenkaart uitdrukkelijk regelen (punten 51-52);
- voor wat de identiteitskaarten afgeleverd door ambassades en consulaire posten betreft moet de regelgeving worden aangepast (punt 54) en een DPIA worden verricht (punt 55);
- preciseren hoe lang de kopie van het attest van verlies, diefstal of vernietiging door de Helpdesk van het Rijksregister wordt bijgehouden (punt 62);
- preciseren wat er met de identiteitskaart/vreemdelingenkaart gebeurt die wordt ingeleverd nadat ze als gestolen of verloren werd aangegeven (punt 64);

↳ vestigt er de aandacht op dat:

- het aangewezen is dat de gebruikte technologie van de chip wordt herbekeken (punten 18, 67 – 70);

vooral in productie te gaan moet het hele proces m.b.t. de aanmaak van de identiteitskaart grondig herbekeken worden in functie van de vaststellingen in de door de Autoriteit verrichte technische analyse (punt 65);

- het louter "lezen" van de vingerafdrukken zoals voorzien is in de wet, niet toelaat een vergelijking te maken (punt 47).

(get.) An Machtens  
Wvd. Administrateur

(get.) Willem Debeuckelaere  
Voorzitter,  
Directeur Kenniscentrum