Advies nr. 106/2018 van 17 oktober 2018

Betreft: Advies uit eigen beweging - Hoorzitting van de Gegevensbeschermingsautoriteit over een wetsontwerp houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters – DOC 54 3256 - Opvolging van het advies 19/2018 van de CBPL (CO-A-2018-132)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet *van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikel 23 en 26;

Gelet op het verslag van de heer Willem Debeuckelaere;

Brengt op 17 oktober 2018 het volgend advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Commissie Binnenlandse Zaken van het Parlement heeft op 16 oktober 2018 de Gegevensbeschermingsautoriteit uitgenodigd voor een hoorzitting over het wetsontwerp houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters – DOS 54 3256.

2. De gegevensbeschermingsautoriteit sprak zich in haar advies nr. 19/2018 van 28 februari 2018 uit over een voorontwerp van wet houdende diverse bepalingen “Binnenlandse Zaken".

3. Aangezien dit wetsontwerp maatregelen bevat die een belangrijke impact hebben voor de rechten en vrijheden van betrokkenen brengt de gegevensbeschermingsautoriteit uit eigen beweging het huidige advies uit teneinde het gevolg te onderzoeken dat werd verleend aan haar voormeld advies 19/2018. Op vele punten volgt het wetsontwerp houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters (hierna "het wetsontwerp") het advies 18/2018 van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL). Gelet op de korte tijd waarover de Gegevensbeschermingsautoriteit (GBA) beschikt, beperkt onderhavig advies zich tot het behandelen van de punten van het advies 18/2018 van de CBPL die niet werden gevolgd, zonder noodzakelijk te streven naar exhaustiviteit, alsook tot opmerkingen over nieuwe bepalingen die een negatieve impact vertonen voor de betrokkenen wat betreft de bescherming van hun fundamenteel recht op bescherming van persoonsgegevens.

4. De aandacht van de parlementsleden wordt in het bijzonder gevestigd op artikel 27 van het wetsontwerp dat voorziet in de registratie van de vingerafdrukken op de chip van de elektronische identiteitskaarten. Gelet op de impact van deze maatregel op het grondrecht op de bescherming van persoonsgegevens, werd een specifiek hoofdstuk hieraan gewijd. Het volgt aan het einde van dit advies.

II. ONDERZOEK TEN GRONDE

5. Uit artikel 2, § 2 van het wetsontwerp blijkt dat nieuwe subregisters kunnen worden gecreëerd door het Rijksregister (hierna "RR"). De formulering van deze bepaling voldoet niet aan de criteria inzake voorzienbaarheid en kwaliteit van wetten die elke verwerking van persoonsgegevens omkaderen en zoals vereist door het Europees Hof voor de Rechten van de Mens. **Artikel 2,§ 2 moet expliciet bepalen welke deze subregisters zijn,** andere dan deze die reeds vermeld

zijn in artikel 2 § 1 van het ontwerp van WRR (bevolkingsregisters, vreemdelingenregister, wachtregister en consulaire registers) en in artikel 6bis van de wet van 19 juli 1991 betreffende de bevolkingsregisters (Register van identiteitskaarten en vreemdelingenkaarten). **Volgens de uitleg opgenomen in de Memorie van toelichting lijkt het te gaan om het Protocolregister en het nieuwe subregister,** gecreëerd door onderhavig wetsontwerp, het **register van de personen die vermeld worden in een akte van de burgerlijke stand**.

6. Betreffende de creatie van dit nieuwe **register van de personen die vermeld worden in een akte van de burgerlijke stand, bestaat er enige vaagheid bij verschillende aspecten; wat moet worden verbeterd om te beantwoorden aan de gevraagde kwaliteitsvereiste**:
    a. **De betrokken akten van burgerlijke stand** dienen **limitatief** te worden **gepreciseerd.**

    b. Bovendien **dient de Verantwoording van de creatie van dit laatste register duidelijk te worden opgenomen in de Memorie van Toelichting zo niet kunnen de legitimiteit en de proportionaliteit ervan niet worden onderzocht.**
        i. **Hoe kan het feit vermeld te worden in een akte van de burgerlijke stand de vermelding van de betrokkene in het RR verantwoorden in het licht van de doeleinden van het Rijksregister?**
        ii. **A priori lijkt de bestaansreden van de inschrijving van een persoon in het Rijksregister te liggen in de herhaaldelijke contacten die deze persoon zal hebben met de Belgische publieke overheden. Is aan dit criterium voldaan voor elke persoon die vermeld wordt in een akte van de burgerlijke stand?**

    c. Naast het probleem van het ontbreken van een concrete verantwoording voor de creatie van dit nieuwe register**, beschrijft ontwerpartikel 2, § 4, 3° van de WRR de nieuwe categorieën personen die in dit register moeten worden opgenomen op een vage en moeilijk uitvoerbare wijze** (*« de gehuwde personen* ***of de personen die van plan zijn in het huwelijk te treden (vaag en niet-controleerbaar criterium)*** *met een in het Rijksregister ingeschreven persoon* de samenwonende personen **(feitelijk of wettelijk?)** *of* ***de personen die van (plan zijn wettelijk te gaan samenwonen (vaag en niet-controleerbaar criterium)*** *met een in het Rijksregister ingeschreven persoon,* ***of de personen die het voorwerp uitmaken van een*** **erkenning, (over welke soort erkenning heeft men het?)** *maar niet beschikken over een identificatienummer in het*

Rijksregister van de natuurlijke personen ») In het licht van artikel 22 van de Grondwet dient niet de Koning maar de wetgever op exhaustieve en welbepaalde wijze de personen te bepalen die betrokken zijn bij een inschrijving in dit centraal register.

d. Dezelfde opmerkingen kunnen eveneens gemaakt worden bij artikel 5 van het wetsontwerp dat een nieuw artikel 2ter invoegt in de WRR " Worden vermeld in het Rijksregister, vanaf de door de minister bevoegd voor Binnenlandse Zaken vastgelegde datum, de natuurlijke personen die vermeld worden in een akte van de burgerlijke stand opgemaakt door een ambtenaar van de burgerlijke stand, maar die niet het voorwerp uitmaken van een inschrijving of een vermelding in het Rijksregister van de natuurlijke personen in een andere hoedanigheid." **Welke zijn de betrokken akten van de burgerlijke stand en met welke verantwoording?**

e. Volgens artikel 9 van het wetsontwerp zullen de gegevens van dit register ("Burgerlijke staat") enkel bewaard worden voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of statistische doeleinden in het algemeen belang. Het betreft hier **een contradictie met artikel 2 van de WRR** dat andere doeleinden vermeldt waarvoor de gegevens van het RR mogen worden aangewend. Dit punt dient te worden opgehelderd (bovenop de voormelde noodzakelijke verantwoordingen).

f. Hetzelfde artikel preciseert de gegevens van deze personen die zullen worden opgenomen in het Rijksregister, doch op deels variabele wijze, te weten de gegevens bedoeld in artikel 3, 1ste lid, 1° en 3° van de WRR en de andere gegevens bedoeld in artikel 3 van de WRR voor zover zij vermeld zijn in de desbetreffende akte van de burgerlijke stand. Dit **is niet verenigbaar met de kwaliteits- en voorzienbaarheidsvereisten van het EHRM** en zou strijdig kunnen bevonden worden met artikel 10 van de Grondwet. De persoonsgegevens die gecentraliseerd zullen worden in dit register moeten op limitatieve wijze door de wet worden bepaald.

7. Artikel 10 van het wetsontwerp wijzigt artikel 5 van de WRR om dit aan te passen ingevolge de opheffing van het Sectoraal comité in de schoot van de Commissie voor de bescherming van de persoonlijke levenssfeer. Voortaan zal de minister van Binnenlandse Zaken instaan voor de **toegangsmachtigingen tot het Rijksregister en het gebruik van het Rijksregisternummer**; wat overeenstemt met zijn rol van verwerkingsverantwoordelijke voor dit register.

a. **Het wetsontwerp verwijst in meerdere artikelen** (cf. onder meer art. 10 en 11)**, naar de voorwaarden en modaliteiten van de machtiging voor toegang tot het RR,** ***« voorzien in § van ontwerpartikel 5 § 1 »***. **Welnu, deze voorwaarden staan in ontwerpartikel 15 van de WRR en zijn verminderd ten opzichte van de voorwaarden waarin momenteel wordt voorzien in de WRR in de alinea's 2 en 3 van artikel 5. Enerzijds dient deze verwijzing te worden verbeterd** (door eveneens het toekomstige artikel 15 van de WRR te beogen) **en anderzijds door de voorwaarden en modaliteiten** van de machtiging bedoeld in ontwerpartikel 15 van de WRR aan te vullen met de **woorden "de verificatie of de toegang tot de gevraagde gegevens en het gevraagde gebruik van het Rijksregisternummer conform de AVG zijn".** Het gaat om een voorrecht van de Minister van Binnenlandse Zaken als verwerkingsverantwoordelijke van het Rijksregister.

b. **Betreffende de controle op de veiligheidsmaatregelen ingevoerd door de gebruikers van het Rijksregister, verduidelijkt de memorie van toelichting dat de Minister ter zake geen enkele voorafgaande controle zal uitvoeren en dat het gaat om een opdracht van de Gegevensbeschermingsautoriteit.** Ongeacht of het voor de Gegevensbeschermingsautoriteit bij de uitoefening van haar controlebevoegdheden is of voor de Minister van Binnenlandse Zaken bij de uitoefening van zijn verificatiebevoegdheid van de voorwaarden om gemachtigd te worden voor toegang tot de gegevens van het Rijksregister, is het een feit dat **de middelen die te hunner beschikking moeten gesteld worden om ter plaatse de door** alle **gebruikers van het Rijksregister** toegepaste **veiligheidsmaatregelen te onderzoeken zeer hoogstaand en** duur zouden moeten zijn.

De wetgever dient dus expliciet de minimale veiligheidsvereisten te bepalen die van de gebruikers van het Rijksregister worden geëist. Dit zal leiden tot een duidelijke gedragslijn ter zake en hen responsabiliseren wat betreft de te nemen maatregelen. Hiertoe zou de wetgever zich bijvoorbeeld kunnen laten inspireren door de formulieren die werden gebruikt door het Sectoraal comité van het Rijksregister **en van de machtigingaanvragers een verklaring op eer eisen dat zij voldoen aan de volgende, in de WRR over te nemen minimale voorwaarden:** (1) De risico's die de verwerkte persoonsgegevens lopen, evalueren en de daarmee verbonden beveiligingsbehoeften vaststellen, (2) Een geschreven document – het beveiligingsbeleid – opstellen waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging worden omschreven, (3) Alle

mogelijke dragers die de verwerkte persoonsgegevens bevatten, identificeren, (4) De interne en externe personeelsleden die bij de verwerking van persoonsgegevens betrokken zijn, ten aanzien van de verwerkte gegevens inlichten over de vertrouwelijkheids- en beveiligingsverplichtingen die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsbeleid, (5) passende beveiligingsmaatregelen nemen om een niet-gemachtigde of onnodige fysieke toegang te verhinderen tot de dragers die verwerkte persoonsgegevens bevatten, (6) de noodzakelijke maatregelen nemen om elke fysieke schade die de verwerkte persoonsgegevens in gevaar zouden kunnen brengen, te verhinderen, (7) maatregelen nemen om de netwerken te beveiligen waaraan apparatuur is gekoppeld die persoonsgegevens verwerkt, (8) een actuele lijst opmaken van de verschillende bevoegde personen die in het kader van de verwerking toegang hebben tot de persoonsgegevens alsook van hun respectieve toegangsniveau (creatie, raadpleging, wijziging, vernietiging), (9) een logische beveiliging invoeren via een mechanisme voor toegangsmachtiging dat ontworpen is zodat de verwerkte persoonsgegevens en de verwerkingen die betrekking hebben op deze gegevens uitsluitend toegankelijk zijn voor personen en toepassingen die daartoe uitdrukkelijk gemachtigd zijn, (10) een loggingsysteem invoeren dat permanente , opsporing en analyse mogelijk maakt van de toegang die personen en logische entiteiten gehad hebben tot de verwerkte persoonsgegevens, (11) het voorzien van een controle op de geldigheid en de efficiëntie in de tijd van de geïmplementeerde technische of organisatorische maatregelen, (12) het invoeren van noodprocedures voor het beheren van veiligheidsincidenten met verwerkte persoonsgegevens, (13) het samenstellen en bijwerken van voldoende documentatie met betrekking tot de organisatie van de informatieveiligheid in het raam van de bedoelde verwerking.

c. **Ten slotte dient de vereiste van voorafgaande machtiging bij Koninklijk besluit gecoördineerd te worden met artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens** die bepaalt dat "Tenzij anders bepaald in bijzondere wetten, in uitvoering van artikel 6.2 van de Verordening formaliseert de federale overheid, wanneer zij op basis van artikel 6.1.c) en e), van de Verordening persoonsgegevens doorgeeft aan enig andere overheid of privéorgaan, voor elke type van verwerking deze doorgifte aan de hand van een **protocol** dat tot stand komt tussen de initiële verwerkingsverantwoordelijke en de verwerkingsverantwoordelijke ontvanger van de gegevens".

8. Ontwerpartikel 5, §2 van de WRR verleent aan de Minister de bevoegdheid om, **via de diensten van het RR, de toegangen te machtigen tot de bevolkingsregisters**. Er wordt verduidelijkt, zoals reeds momenteel het geval is in de WRR, dat deze gegevens niet worden bewaard in het Rijksregister.

   Deze **fictie dient gecorrigeerd** te worden aangezien het onmogelijk is om bij een gegevensstroom als tussenpersoon op te treden zonder de bedoelde gegevens gedurende een minimale tijdsspanne te bewaren. Volgens de memorie van Toelichting dient deze formulering zodanig begrepen te worden dat de via de diensten van het Rijksregister geraadpleegde gegevens van de bevolkingsregisters niet beschouwd mogen worden als *"wettelijke" gegevens in de zin van de WRR.* **Wat betekent dit concreet en welke zijn de concrete consequenties inzake verwerking en toegankelijkheid van deze gegevens?**

9. **Ontwerpartikel 5ter van de WRR voorziet in de openstelling van het Rijksregister voor de privésector voor de bijwerking van hun bestanden of databanken van hun cliënteel mits betaling van de diensten van het Rijksregister** .

   a. De meerderheid van de opmerkingen die de CBPL dienaangaande maakte werden gevolgd met uitzondering van deze betreffende de noodzaak om het invoeren van minimale veiligheidsmaatregelen op te leggen aan de private en openbare instellingen die op deze basis de wijzigingen van het Rijksregister zullen ontvangen. Ontwerpartikel 5ter, §2, 6° voorziet enkel in de verplichting om een functionaris voor gegevensbescherming aan te wijzen alsook een "gegevensveiligheidsplan" permanent ter beschikking van de Gegevensbeschermingsautoriteit te houden zonder verdere precisering. **Gelet op het totaal ontoereikende karakter van deze laatste maatregel dient de wetgever in de plaats de minimale veiligheidsmaatregelen te bepalen waaraan deze instellingen moeten voldoen om de gegevenswijzigingen te ontvangen. In dit verband wordt verwezen naar punt 7.b. hiervoor.** Er zou door de wetgever kunnen worden voorzien in een verklaring op eer betreffende de invoering van deze maatregelen.

   b. **Ontwerpartikel 5ter, §2, 3° zou moeten gecorrigeerd worden aangezien de onmiddellijke vernietiging eisen van de basisidentificatiegegevens van de betrokkene bij de beëindiging van de overeenkomst potentieel strijdig is met de AVG.** Bij wijze van voorbeeld, in geval van betwisting met betrekking tot deze overeenkomst kan een langere bewaring conform de AVG worden verantwoord. De woorden "de gegevens moeten bij de beëindiging van de overeenkomst onmiddellijk vernietigd worden" zouden moeten worden geschrapt.

c. **Om het effectieve karakter te verzekeren van de verplichting voor de betrokken instellingen om de diensten van het RR in te lichten over de beëindiging van de contractuele overeenkomst waarvoor hen de wijzigingen van de RR-gegevens, voorzien in artikel 5ter, §3 worden meegedeeld, dient in een strafrechtelijke sanctie te worden voorzien ingeval van niet-naleving.** Deze verplichting is belangrijk in het licht van het recht op bescherming van persoonsgegevens aangezien zij het legitieme karakter van de bedoelde gegevensstroom in de tijd verzekert. Zonder deze specifieke strafrechtelijke sanctie bestaat er een zeker risico dat deze verplichting dode letter blijft en dat de diensten van het Rijksregister zonder rechtmatige basis zullen doorgaan met het meedelen aan deze instellingen van niet-relevante gegevens.

Dezelfde opmerking geldt voor ontwerpartikel 5ter, §5 van de WRR dat stelt dat de gegevens die op basis van dit ontwerpartikel 5ter ter beschikking van de instellingen worden gesteld niet verkocht noch gecommuniceerd mogen worden aan derden, noch gebruikt worden voor reclamedoeleinden.

d. **Het ontwerpartikel 5ter § 4 van de WRR voorziet dat** "*De lijst van alle instellingen die gemachtigd zijn door natuurlijke personen om mededeling te krijgen van de wijzigingen aangebracht aan de gegevens van het Rijksregister van de natuurlijke personen, alsook van de doeleinden waarvoor die wijzigingen meegedeeld worden, wordt opgemaakt, bijgewerkt en beschikbaar gesteld op de internetsite van het Rijksregister.* » **.** Aangezien de vaststelling van deze instellingen en de voormelde doeleinden voor mededeling van de gegevens gekoppeld zijn aan de toestemming van iedere betrokkene, mag deze lijst enkel toegankelijk zijn voor iedere fysieke betrokkene en niet openbaar op het internet. Indien het de intentie van de wetgever is om de namen bekend te maken van de instellingen die potentieel van dit systeem gebruik wensen te maken, dient deze bepaling in die zin geherformuleerd te worden opdat zij de intentie van de wetgever correct zou weergeven. **In de huidige formulering vormt de door ontwerpartikel 5ter § 4 van de WRR geplande publicatie een verwerking van persoonsgegevens die strijdig is met de AVG**.

10. Teneinde een correct minimaal beveiligingsniveau door de gebruikers van het Rijksregister te verzekeren **dient ontwerpartikel 10 van de WRR de minimaal vereiste veiligheidsmaatregelen te preciseren.** Er wordt verwezen naar punt 7.b. van onderhavig advies.

11. Het wetsontwerp schrapt het huidige artikel 12, § 2, van de WRR dat aan iedere begunstigde van een machtiging voor toegang tot het RR oplegt een nominatieve lijst op te stellen en bij te werken van hun organen of aangestelden die, omwille van hun bevoegdheden, gemachtigd zijn om toegang te hebben tot het RR. **De Memorie van Toelichting bevat geen enkele verantwoording voor deze schrapping hoewel deze verplichting de gebruikers van het Rijksregister verplicht om hun personeelsleden die gemachtigd worden om het Rijksregister te raadplegen tot het strikt noodzakelijke te beperken.**

12. De Autoriteit stelt tot haar genoegen de invoering vast van de wettelijke verplichting tot het correct bijhouden van de loggings van de toegangen door de gebruikers tot het Rijksregister alsook van de bestraffing van de niet-naleving van deze verplichting. Dit zal in belangrijke mate de situatie verbeteren waarmee de CBPL herhaaldelijk werd geconfronteerd tijdens controles ingevolge vermoedens van illegaal gebruik van gegevens van het Rijksregister; vaak stelden de verwerkingsverantwoordelijken dat zij bij gebrek aan loggings onmogelijk konden nagaan wie de gegevens had gebruikt.

    Bovenop het verplichten van deze loggings voorziet **ontwerpartikel 17, 5de lid van de WRR** in het bijhouden door de diensten van het RR van een register met de raadplegingen door gebruikers en uitgevoerde mededelingen met opgave van de identificatie van de gebruiker die toegang had tot de gegevens, de geraadpleegde gegevens en datum en uur van de raadpleging. Zoals voor elke verwerking van persoonsgegevens die specifiek wordt omkaderd door de wet dient **het concrete doeleinde te worden vermeld waarvoor dit interne register wordt gecreëerd**.

13. Aangaande artikel 27 van het wetsontwerp tot wijziging van artikel 6 van de van 19 juli 1991 betreffende de bevolkingsregisters (wet van 1991) dat onder meer voorziet in de invoering van de vingerafdrukken, wordt verwezen naar het hoofdstuk van onderhavig advies dat specifiek aan dit onderwerp wordt gewijd (punten 19 en volgende).

14. **Ontwerpartikel 6 §4 van** de wet van 1991 **regelt het lezen en de registratie van de gegevens van de identiteitskaart** door te stellen dat alle hierop voorkomende gegevens met uitzondering van de foto, het Rijksregisternummer en van de vingerafdrukken - kunnen gelezen en/of opgenomen worden, in overeenstemming met de bepalingen inzake de bescherming van de persoonlijke levenssfeer en de persoonsgegevens. Er wordt verduidelijkt dat de foto en het Rijksregisternummer slechts mogen worden gebruikt mits wettelijke machtiging of bij ministerieel besluit.

    De Memorie van toelichting preciseert dat de wetgever de vaststelling van de instellingen die gemachtigd worden om de foto van de identiteitskaart te lezen niet

kan opleggen - zoals dit zal gebeuren voor het lezen van de afbeelding van de vingerafdrukken- en rechtvaardigt dit standpunt op basis van het feit dat de foto op de identiteitskaart met het blote oog zichtbaar is.

Deze verantwoording overtuigt niet. **Aangezien het geautomatiseerd lezen en de registratie van de foto van de identiteitskaart een bijzonder risico genereren inzake identiteitsfraude oordeelt de Autoriteit dat de overheden die gemachtigd worden om over te gaan tot dergelijke verwerkingen limitatief zouden moeten worden bepaald door de wet en dat specifieke technische beveiligingsmaatregelen het geautomatiseerd lezen van de foto van de identiteitskaart zouden moeten omkaderen.**

15. Ontwerpartikel 6 §4 2de lid in fine van de wet van 1991 conditioneert het uitlezen en het gebruik van de elektronische identiteitskaart aan de noodzaak om vooraf een specifieke en geïnformeerde toestemming te verkrijgen van de titularis en het 4de lid van diezelfde bepaling stelt dat "*zonder afbreuk te doen aan artikel 1 van het KB van 25/03/2003, de houder van de elektronische identiteitskaart kan weigeren dat zijn gegevens gelezen en/of opgenomen zouden worden, behalve in de door de Koning bij een in Ministerraad overlegd besluit bepaalde gevallen* ». **Considerans 78 van het advies van de CBPL werd niet gevolgd.** De regering leest het KB van 25 maart 2003 op een totaal andere wijze dan de CBPL door te stellen dat dit KB eveneens van toepassing is voor de actoren van de privésector.

Welnu, de Autoriteit herhaalt dat dit KB van 25 maart 2003 (en meer bepaald zijn artikel 1) werd genomen in uitvoering van artikel 6, § 7 van de Wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten dat aan de Koning de bevoegdheid verleent om "**de overheden en openbare ambtenaren te bepalen op wiens vraag de identiteitskaart moet worden getoond**"; wat het standpunt van de CBPL versterkt bij haar opmerking in cons.78 : in tegenstelling tot wat wordt gesteld in de Memorie van Toelichting is dit KB niet van toepassing op de privésector.

Bijgevolg, volgens de opmaak van ontwerpartikel 6 § 4 van de wet van 1991 zullen alle actoren van de privésector de voorafgaande toestemming moeten vragen van de betrokkene om de identiteitskaart van een persoon te lezen. **Dit dreigt de werking van de actoren van de privésector die gehouden zijn door een wettelijke bepaling (voorafgaand aan het huidig wetsontwerp) om de identiteit in te zamelen van personen aan de hand van hun identiteitskaart, sterk te bemoeilijken**. Teneinde dit te vermijden, dient op het einde van het 2de lid van het toekomstige art. 6. §4 te worden toegevoegd "Behoudens strijdige wettelijke bepaling".

Bovendien, naast de wettelijke bepalingen die voorzien in het lezen van de identiteitskaart, kunnen bepaalde soorten contracten (in het algemeen synallagmatische contracten met, voor zover nodig, opeenvolgende prestaties) vereisen dat men zich vergewist van de correcte identiteit van een betrokkene bij de afsluiting ervan en een legitieme basis vormen om te vragen dat de identiteitskaart wordt getoond. Welnu, door de optie van de toestemming hiertoe te beperken, dreigt dit eveneens sommige actoren van de privésector in de onmogelijkheid te plaatsen om de identiteit van hun contractant via deze weg te controleren. In dit verband wordt verwezen naar **de Aanbeveling uit eigen beweging van de CBPL nr. 03/2011** over het nemen van een kopie van de identiteitskaart en over het gebruik en de elektronische lezing ervan.

16. **Artikel 28** van het wetsontwerp verleent aan de Minister van Binnenlandse Zaken de bevoegdheid **om toegang te verlenen tot het Register van de identiteitskaarten** doch zodoende breidt hij **eveneens het aantal potentiële begunstigden -die momenteel zijn beperkt tot de openbare overheden - uit en dit zonder enige verantwoording**.

    In de mate dat deze Registers van de identiteitskaarten gevoeliger zijn ten opzichte van het Rijksregister, ingevolge de gegevens die zij bevatten en gelet op het risico op fraude en identiteitsdiefstal dat kan voortvloeien uit een onterecht gebruik van de identiteitsfoto van de kaart, dienen deze registers een beperkte toegang te kennen ten opzichte van het Rijksregister. Een logische optie zou erin bestaan hun toegankelijkheid te beperken tot de bevoegde autoriteiten met het oog op de opsporing van strafbare feiten, onderzoek en vervolging of de tenuitvoerlegging van strafrechtelijke sancties.

17. Artikel 29 van het wetsontwerp wijzigt artikel 6ter van de wet van 1991 in die zin dat het voortaan niet meer in de wet is voorzien dat de elektronische functies van gestolen of verloren identiteitskaarten rechtstreeks door de gemeente worden geschorst of buiten dienst gesteld. De vaststelling van deze nadere regels wordt voortaan verleend aan de Koning. Het nut om dit over te laten aan de Koning is niet duidelijk. Dit zou rechtstreeks in de wet moeten worden voorzien. Het is belangrijk dat deze functies meteen worden geschorst ingeval van diefstal of verlies. Bovendien omvat de delegatie aan de Koning in ontwerpartikel 6ter, 4de lid eveneens de vaststelling van de autoriteiten bij wie aangifte van de diefstal moet worden gedaan terwijl het 1ste lid van ontwerpartikel 6ter dit reeds bepaalt.

18. Wat artikel 30 van het wetsontwerp betreft over de toepassing van **Checkdoc**, **werd het advies van de Commissie** - die aanbeval te eisen dat de gebruikers van deze toepassing die toegang

zouden hebben tot de persoonsgegevens van de burgers (informatie of hun identiteitskaart nog al dan niet geldig is) vooraf zouden worden geïdentificeerd en geauthenticeerd - **niet gevolgd**.

De Memorie van Toelichting vermeldt de onmogelijkheid om te identificeren en te authenticeren gezien de noodzaak van een zo ruim mogelijke toegang tot de dienst. Bijgevolg **kunnen de burgers onmogelijk de bestemmelingen kennen van hun persoonsgegevens** (informatie of hun identiteitskaart of paspoort nog al dan niet geldig is - werd verloren of gestolen of is vervallen) **die deze checkdoc dienst gebruiken, indien zij een vraag om toegang indienen**; **wat onaanvaardbaar is**.

Bovendien voorzag de versie van het voorontwerp van wet van dit artikel dat de diensten van het Rijksregister gedurende 10 jaar de gegevens zouden bewaren vanaf de datum van verificatie van documenten waarvan de geldigheid werd nagegaan alsook de gebruikers van de checkdoc informaticatoepassing. **Het is belangrijk dat het wetsontwerp eveneens deze precisering herneemt ten behoeve van de voorzienbaarheid ten opzichte van de gebruikers van checkdoc**.

Indien deze opmerkingen niet worden gevolgd is het op z'n minst belangrijk dat vooraf **een risicobeoordeling wordt uitgevoerd van een dergelijke openstelling van de checkdoc toepassing** (risico op identiteitsdiefstal, vervalsing van identiteitsdocumenten...) en dat de gekozen optie wordt verantwoord op basis van de conclusies van deze risicoanalyse.

19. **Betreffende de registratie van de vingerafdrukken van de volledige bevolking op de chip van de elektronische identiteitskaart (artikel 27 van het wetsontwerp)**

---

20. Het wetsontwerp heeft de kritiek die dienaangaande door de gegevensbeschermingsautoriteit in haar advies 19/2018 van 28 februari 2018 werd geformuleerd (punten 62 tot 71) niet verholpen.

21. Zelfs indien is voorzien dat de vingerafdrukken enkel zullen bewaard worden op de chip van de elektronische identiteitskaart, wordt de aandacht van de parlementariërs gevestigd op de volgende punten.

22. In tegenstelling tot wat is vermeld in de Memorie van Toelichting, heeft de Europese Commissie geen aanbeveling geformuleerd over de registratie van de vingerafdrukken op de identiteitskaarten doch enkel een voorstel **van EU Verordening van de Europese Commissie**

neergelegd op 17 april 2018 over de registratie van biometrische gegevens op de Europese identiteitskaarten. Dit voorstel van EU Verordening dat - in tegenstelling tot het thans besproken Belgische wetsontwerp evenwel expliciet op limitatieve wijze de doeleinden verduidelijkt waarvoor biometrische gegevens (gelaatsafbeelding en vingerafdruk) zullen kunnen worden gebruikt - heeft op zijn beurt **een zeer kritisch advies gekregen van de Europese Toezichthouder voor gegevensbescherming**[1] **en** dient nog verder het Europese wetgevende proces te doorlopen.

23. Er staat in de Memorie van toelichting **nog steeds geen reële verantwoording voor de geplande maatregel** hoewel dit door de Gegevensbeschermingsautoriteit werd gevraagd. Onze identiteitskaart is reeds uitgerust met voorzieningen tegen vervalsing (hologram, ...) alsook met een biometrisch element (gelaatsafbeelding). **Hoezo is dit concreet ontoereikend? Over welke statistieken beschikt de regering die de geplande maatregel staven?**

24. In zijn voormeld advies merkte de Europese Toezichthouder voor gegevensbescherming (EDPS) op dat **de statistieken niet pleiten in het voordeel van het voorstel van de Europese Commissie** dat in dezelfde lijn ligt als dat van de regering. Statistieken van het Europese Grens- en kustwachtagentschap (Frontex) tonen slechts 38.870 gevallen van frauduleus gebruik van nationale identiteitskaarten over de periode 2013-2017. Bovendien stelt men een daling vast van minstens 11% sinds 2015 van het frauduleus gebruik van verblijfsdocumenten door personen uit derde landen.

25. **De door de regering vooropgestelde gelijkstelling van de identiteitskaarten met de paspoorten om deze maatregel te verantwoorden is onaanvaardbaar**: zelfs indien de identiteitskaarten ook als reisdocument kunnen gebruikt worden binnen de Europese Unie, worden zij momenteel niet systematisch gecontroleerd gelet op het recht op vrij verkeer binnen de Europese Unie. Bovendien, en in tegenstelling tot de paspoorten, bieden de identiteitskaarten tal van andere gebruiksmogelijkheden (toepassingen van de privésector,...). Dit punt werd eveneens opgemerkt door de EDPS in zijn advies. **Gelet op de verschillen tussen de identiteitskaarten en de paspoorten kan de invoering van veiligheidselementen, die in het raam van paspoorten als passend kunnen worden beschouwd, niet automatisch gebeuren voor de identiteitskaarten maar vereist dit een grondige analyse en overweging die niet lijken te hebben plaatsgevonden**.

[1] Advies 07/2018 van 10 augustus 2018 van de EDPS inzake het voorstel voor een verordening betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en andere documenten

26. **Blijkbaar werd geen enkele gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd over het ontwerp om de vingerafdrukken van de burgers te registreren de chip van de elektronische identiteitskaart.** De Memorie van Toelichting vermeldt enkel dat "een **"PIA" zullen worden uitgevoerd.**

    Welnu, de geplande maatregel dient krachtens artikel 35.2.b van de AVG het onderwerp te vormen van een DPIA en dit voorafgaand aan zijn wettelijke omkadering aangezien het zeer waarschijnlijk is dat deze analyse aanleiding geeft tot andere maatregelen of - zoals het geval was met het voorstel van EU Verordening van de Europese Commissie - tot het beperken van het verplichte karakter van de registratie van biometrische gegevens op identiteitskaarten tot de gelaatsafbeelding van de houder en de verduidelijking van het facultatieve karakter van de registratie van de vingerafdrukken[2].

27. Het verbod op de verwerking van biometrische gegevens kan slechts worden opgeheven op basis van artikel **9.2.g van de AVG** die niet alleen vereist dat de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, maar eveneens dat **de evenredigheid met het nagestreefde doel wordt gewaarborgd, en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkenen**. **Deze zijn momenteel ontoereikend** :

    a. De keuze van de regering om **het digitale beeld van de vingerafdrukken** in te zamelen en op te slaan op de chip van de kaart vormt volgens de EDPS niet de meest opportune keuze gelet op **het risico van onrechtmatig gebruik** van de identiteit in geval van hacking van de gegevens die voorkomen op de elektronische chip van de kaart[3]. Deze keuze dient dus te worden herzien en **de in de chip van de identiteitskaarten opgeslagen dactyloscopische gegevens beperkt te worden tot een onderverzameling van kenmerken afgeleid uit de vingerafdruk of nog tot biometrische technieken die geen sporen nalaten (handomtrek, bloedvatenstelsel van een vinger...).**

---

[2] Punt 31 van het advies 07/2018 van de Europese Toezichthouder over dit voorstel van Verordening (vrije vertaling) "Na vergelijking van de strategische opties geeft een effectbeoordeling aan dat de optie ID 1) de meest gepaste is om de doelstellingen van verhoging van de veiligheid aan de grenzen en in de schoot van de lidstaten te bevorderen alsook het vrije verkeer. Er dient te worden opgemerkt dat de optie ID 1) die de voorkeur krijgt in het verslag over de effectbeoordeling "een verplichte RFID chip zou integreren met biometrische gegevens (verplichte gelaatsafbeelding, facultatieve vingerafdrukken)" Met andere woorden, de strategische keuze die ondersteund wordt door de effectbeoordeling bij het voorstel zou optioneel voorzien in de opname van de vingerafdrukken en dus niet als verplichte voorwaarde". Zelfs indien de Europese Commissie hiermee duidelijk geen rekening heeft gehouden in haar ultiem voorstel; wat wordt bekritiseerd in het advies van de EDPS (cf. infra).

[3] Zoals aangestipt door de EDPS in zijn advies, "in geval van een fout in de beveiliging zou het beeld van de vingerafdrukken dat opgeslagen is op een verloren of gestolen identiteitsdocument kunnen worden gerecupereerd en op criminele wijze gebruikt om een valse set vingerafdrukken te creëren die zou toelaten misbruik te maken van de identiteit van de houder van de kaart".

b. In plaats van de taak aan de Koning te delegeren om de autoriteiten te bepalen die gemachtigd zullen zijn om de vingerafdrukken te lezen, behoort dit toe aan de wetgever in de formele zin van het woord.
c. **Er dient eveneens in de wet te worden bepaald dat het lezen van deze gegevens slechts toegelaten is om de authenticiteit van de identiteitskaart te verifiëren**. Er dienen in de wet eveneens reeds maatregelen te worden opgenomen om het aantal leestoestellen die toelaten de vingerafdrukken te lezen te beperken.
d. **Welke zijn de specifieke beschermingsmaatregelen die werden genomen om de risico's op hacking van het certificaat van de identiteitskaart dat het beeld van de vingerafdrukken zal bevatten te voorkomen, zowel inzake beveiliging van de chip waarop de gegevens worden opgeslagen als de beveiliging van de toestellen om deze gegevens te lezen?**
e. Welke zijn **de beschermingsmaatregelen voor de tijdelijke databank die de vingerafdrukken op gecentraliseerde wijze zal overnemen gedurende 3 maanden en wie zal de verwerkingsverantwoordelijke zijn?**
f. Tot slot, en zoals aangestipt door de EDPS, zouden **kinderen jonger dan 14 jaar** niet aan deze maatregel mogen worden onderworpen.

OM DIE REDENEN,

Naast de voormelde opmerkingen brengt de Autoriteit **een ongunstig advies** uit over het wetsontwerp, voornamelijk om reden van zijn artikel 27 dat voorziet in de registratie van de vingerafdrukken op de elektronische chip van de identiteitskaarten.

Om de redenen uiteengezet in onderhavig advies (punten 19 en v.), wordt aan de parlementariërs aanbevolen de intrekking te vragen van deze maatregel van het wetsontwerp ingevolge de noodzaak en de wettelijke verplichting, bepaald in artikel 35.3.b van de AVG, om voorafgaandelijk over te gaan tot de effectbeoordeling ervan op de gegevensbescherming en te beschikken over statistieken en concrete elementen die de ontoereikendheid van ons huidige model van identiteitskaart aantonen in de strijd tegen vervalsing van deze kaart aangezien zij reeds beschikt over een biometrisch element (gelaatsafbeelding) en voorzieningen tegen vervalsing (hologram,...).

In plaats van vooruit te lopen op het voorstel van EU Verordening van de Europese Commissie zou het wenselijker zijn te wachten tot dit voorstel het einde van het Europese wetgevende proces bereikt, te meer daar dit voorstel reeds een zeer kritisch advies kreeg vanwege de Europese Toezichthouder voor gegevensbescherming (advies 07/2018 van de EDPS van 10 augustus 2018).

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere