



**Advies nr. 162/2019 van 18 oktober 2019**

**Betreft: advies m.b.t een ontwerp van Koninklijk besluit tot verlening van toegang tot de DABS aan de Dienst Legalisatie en bestrijding documentaire fraude van de Federale overheidsdienst Buitenlandse Zaken (CO-A-2019-169)**

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 Koen Geens, Vice-eersteminister en minister van Justitie belast met de Regie der Gebouwen, ontvangen op 23/08/2019;

Gelet op het verslag van mevrouw Alexandra Jaspar, Directeur van het Kenniscentrum van de Gegevensbeschermingsautoriteit;

Brengt op 18 oktober 2019 het volgend advies uit:

## I. VOORWERP VAN DE AANVRAAG

1. De wet van 18 juni 2018 *houdende diverse bepalingen inzake burgerlijk recht en bepalingen met het oog op de bevordering van alternatieve vormen van geschillenoplossing* paste onder meer een aantal bepalingen van het Burgerlijk Wetboek aan. Een van die aanpassingen bestond in de creatie van de databank voor de akten van de burgerlijke stand (DABS) die voortaan als authentieke bron geldt (artikel 71 *Burgerlijk Wetboek*) voor alle authentieke akten opgemaakt na de inwerkingtreding van de hiervoor vermelde wet van 18 juni 2018, zijnde 31 maart 2019.

2. De taken/doeleinden van de DABS (artikel 72 *Burgerlijk Wetboek*) bestaan onder meer uit:

*"(...) 3° het verzekeren van de dienstverlening aan de burgers, ongeacht waar ze zich bevinden; 4° het vereenvoudigen van administratieve procedures door het verplicht hergebruik van de in de DABS beschikbare akten en gegevens (...)"*.

3. Artikel 78 *Burgerlijk Wetboek* identificeert een aantal beroepsgroepen en instellingen die toegang hebben tot de gegevens van de DABS. Daarnaast biedt artikel 80 *Burgerlijk Wetboek* de Koning de mogelijkheid om onder de voorwaarden die hij bepaalt en na advies van de Autoriteit, andere categorieën van personen, overheden of instellingen aan te duiden om toegang te verlenen indien dit noodzakelijk is voor de uitvoering van hun wettelijke opdrachten. Daarnaast preciseert artikel 80 *Burgerlijk Wetboek* dat de Koning de erin voorziene toegang slechts kan verlenen op voordracht van het beheerscomité van de DABS. Dit comité bracht een gunstig advies uit op 28/05/2019. Deze regeling wijkt af van het algemene regime dat artikel 20 WVG invoerde voor de doorgifte van persoonsgegevens door een federale overheid, namelijk het sluiten van een protocol tussen de verstrekende verwerkingsverantwoordelijke en de ontvangende verwerkingsverantwoordelijke.

4. Het is in uitvoering van dit laatste artikel dat de heer Koen Geens, Vice-eersteminister en minister van Justitie belast met de Regie der Gebouwen, hierna de aanvrager, het ontwerp van koninklijk besluit *tot verlening van toegang tot de DABS aan de Dienst Legalisatie en bestrijding van documentaire fraude van de Federale overheidsdienst Buitenlandse Zaken*, hierna "het ontwerp", voor advies voorlegt. Het ontwerp verleent de Dienst Legalisatie en bestrijding van documentaire fraude leesrechten in de DABS, meer in het bijzonder tot de gegevens van de akten van de burgerlijke stand die noodzakelijk zijn in het kader van een verzoek tot legalisatie of apostille ervan.

## II. TEN GRONDE

### 1. Rechtsgrond

5. Elke verwerking van persoonsgegevens moet steunen op een rechtsgrond in de zin van artikel 6 AVG.

6. De Autoriteit stelt vast dat de door het ontwerp gegenereerde verwerkingen in hoofde van de verwerkingsverantwoordelijke die de gegevens verstrekt, gestoeld zijn op artikel 6.1.e) AVG, namelijk een taak van algemeen belang (zie artikelen 71 en 72 *Burgerlijk Wetboek* - punten 1 en 2). In hoofde van de Dienst Legalisatie en bestrijding van documentaire fraude die de gegevens ontvangt, lijkt de verwerking gestoeld op artikel 6.1.c) of e) AVG.

7. Krachtens de transparantie- en wettelijkheidsbeginselen vervat in artikelen 8 van het EVRM en 22 van de Grondwet, dient de wet duidelijk te bepalen in welke omstandigheden een verwerking van persoonsgegevens is toegestaan<sup>1</sup>, en bijgevolg te bepalen: welke gegevens worden verwerkt, wie de betrokkenen zijn, welke de voorwaarden en doeleinden van de bedoelde verwerking zijn, wat de bewaartermijn van de gegevens is<sup>2</sup> en welke personen toegang hebben<sup>3</sup>. De Autoriteit had al de gelegenheid om deze beginselen in herinnering te brengen<sup>4</sup>. Wanneer de verwerking berust op een rechtsgrond van nationaal recht, eist artikel 6.3, van de AVG specifiek dat de doeleinden ervan in deze rechtsgrond worden gedefinieerd.

8. Artikel 22 van de Grondwet verbiedt de wetgever om af te zien van de mogelijkheid om zelf te bepalen welke inmengingen het recht op eerbiediging van de persoonlijke levenssfeer kunnen beknotten<sup>5</sup>. In deze context is een delegatie aan de Koning "niet in strijd met het wettigheidsbeginsel

<sup>1</sup> In die zin, lees Grondwettelijk Hof, Arrest nr. 29/2018 van 15 maart 2018, punten B.9 en v. en punt punt B.13.3 in het bijzonder.

<sup>2</sup> Het Grondwettelijk Hof heeft erkend dat "de wetgever (...) de bewaring van persoonsgegevens en de duur van die bewaring op een algemene wijze (vermocht) te regelen", Arrest nr. 29/2018 van 15 maart 2018, punt B. 23.

<sup>3</sup> Lees bijvoorbeeld, Grondwettelijk Hof, Arrest nr. 29/2018 van 15 maart 2018, punt B.18, en Grondwettelijk Hof, Arrest nr. 44/2015 van 23 april 2015, punten B.36.1 en v.

<sup>4</sup> Zie het Advies van de Autoriteit nr. 110/2018 van 17 oktober 2018, punten 7-9.

<sup>5</sup> Advies nr. 63.202/2 van 26 april 2018 van de Raad van State gegeven over een over een voorontwerp van wet *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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, Parl.St. Kamer, 54-3185/001, blz 121-122.*

Zie in dezelfde zin volgende adviezen van de Raad van State:

- Advies 26.198/2, op 2 februari 1998 gegeven over een voorontwerp dat geleid heeft tot de wet van 11 december 1998 *tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, Parl.St. Kamer 1997-98, nr. 49-1566/1, 108;*
- Advies 33.487/1/3 van 18 en 20 juni 2002 betreffende een voorontwerp dat geleid heeft tot de wet van 22 augustus 2002 *houdende maatregelen inzake gezondheidszorg, Parl.St Kamer 2002-03, nr. 2125/2, 539;*
- Advies 37.765/1/2/3/4, op 4 november 2004 gegeven over een voorontwerp dat geleid heeft tot de programmawet van 27 december 2004, *Parl.St. Kamer 2004-05, nr. 1437/2.*

voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgelegd<sup>6</sup>". *In casu* bakent artikel 80 *Burgerlijk Wetboek* de bevoegdheid van de Koning nauwkeurig af.

## **2. Doeleinden**

9. Volgens artikel 5.1.b) AVG kan de verwerking van persoonsgegevens enkel uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

10. Artikel 1 van het ontwerp vermeldt uitdrukkelijk het doeleinde waarvoor de toegang wordt gevraagd, namelijk het legaliseren of apostilleren van uittreksels van akten van de burgerlijke stand.

11. Artikel 29, § 3, *Burgerlijk Wetboek* belast de minister van Buitenlandse Zaken of de door hem gemachtigde ambtenaar met het legaliseren van uittreksels en afschriften van akten van de burgerlijke stand zodat men ze in het buitenland kan gebruiken.

12. Ingevolge het Verdrag van Den Haag van 5 oktober 1961 *tot afschaffing van het vereiste van legalisatie van buitenlandse openbare akten*<sup>7</sup>, moeten o.a. Belgische akten van de burgerlijke stand die in een van de andere verdragsluitende partijen moeten worden voorgelegd niet langer gelegaliseerd worden. Het volstaat dat de bevoegde autoriteit een apostille op het stuk aanbrengt die de echtheid van de handtekening, de hoedanigheid waarin de ondertekenaar van het stuk heeft gehandeld en desgevallend de identiteit van het zegel of de stempel op het stuk bevestigt.

13. In uitvoering van artikel 6 van dit verdrag werd de FOD Buitenlandse Zaken, en Ontwikkelingssamenwerking aangeduid als bevoegde autoriteit om apostilles af te geven.

14. In het licht hiervan stelt de Autoriteit vast dat het doeleinde voldoet aan de vereisten van artikel 5.1.b) AVG.

15. Zoals aangestipt in punt 3 vermeldt het besluit dat toegang verleent, ook de voorwaarden waaronder dit gebeurt. Voor het bepalen van deze voorwaarden, kan de aanvrager inspiratie putten uit artikel 20, § 1, tweede lid, WVG dat een opsomming bevat van de elementen die een protocol best

---

<sup>6</sup> Zie eveneens Grondwettelijk Hof, Arrest nr. 29/2010 van 18 maart 2010, punt B.16.1 ; Arrest nr. 39/2013 van 14 maart 2013, punt B.8.1 ; Arrest 44/2015 van 23 april 2015, punt B.36.2; Arrest nr. 107/2015 van 16 juli 2015, punt B.7; Arrest nr. 108/2017 van 5 oktober 2017, punt B.6.4 ; Arrest nr. 29/2010 van 15 maart 2018, punt B.13.1, Arrest nr. 86/2018 van 5 juli 2018, punt B.7.2.; Advies van de Raad van State nr. 63.202/2 van 26 april 2018, punt 2.2.

<sup>7</sup> Werd door België getekend op 10 maart 1970 en geratificeerd op 11 december 1975 (BS 21/07/1983).

regelt. De vermelding van de wettelijke grondslag voor de doorgifte is er één van<sup>8</sup>. Het in het ontwerp nagestreefde doeleinde kadert in een specifieke wettelijke opdracht toevertrouwd aan de FOD Buitenlandse Zaken. De Autoriteit beveelt dan ook aan om in het ontwerp een uitdrukkelijke verwijzing op te nemen naar de bepalingen die deze opdracht aan de FOD Buitenlandse Zaken toevertrouwen.

### ***3. Proportionaliteit***

16. Artikel 5.1.c), AVG bepaalt dat persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de beoogde doeleinden ('minimale gegevensverwerking').

17. Het ontwerp verleent toegang tot de gegevens van de akten van de burgerlijke stand die noodzakelijk zijn in het kader van een legalisatie of apostille ervan (artikel 2 van het ontwerp). Eigenlijk komt dit neer op een parafrasering van artikel 5.1.c) AVG.

18. Dergelijke algemene formulering laat de Autoriteit niet toe om enige uitspraak te doen over de proportionaliteit. Het ontwerp moet op dit punt worden aangevuld<sup>9</sup>.

19. Als men vaststelt dat een apostille de echtheid van de handtekening, de hoedanigheid waarin de ondertekenaar van het stuk heeft gehandeld en in voorkomend geval de identiteit van het zegel of de stempel bevestigt (artikel 5, tweede lid, van het Verdrag van Den Haag van 5 oktober 1961), dan stelt zich de vraag waarom het ontwerp niet opsomt welke gegevens er de facto nodig zijn om deze echtheid te kunnen bevestigen? Idem dito voor wat de legalisatie betreft.

### ***4. Betrokkenen***

20. Uit het ontwerp blijkt niet welke (groep) personen de toegang viseert. In de DABS zijn alle akten van de burgerlijke stand en hun administratieve bijwerkingen opgenomen (artikel 71 *Burgerlijk Wetboek*). Potentieel wordt dus iedereen die in België woont, geïdendeerd. Als men echter naar de data kijkt die nodig zijn om een apostille af te leveren, dan lijkt de FOD Buitenlandse zaken alleen nood te hebben aan de gegevens van de instrumenterende ambtenaar. Bijgevolg zouden de betrokkenen beperkt zijn tot deze beroepsgroep.

21. Het ontwerp moet op dit punt worden verduidelijkt.

---

<sup>8</sup> Artikel 20, § 1, tweede lid, 7°, WVG.

<sup>9</sup> Voor wat een protocol betreft: de categorieën van doorgegeven persoonsgegevens en hun formaat (artikel 20, § 1, tweede lid, 5°, WVG)

## **5. Bewaartermijn**

22. Krachtens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

23. De Autoriteit stelt vast dat het ontwerp niet voorziet in enige bewaartermijn van de te verwerken persoonsgegevens in hoofde van de FOD Buitenlandse Zaken. In het licht van artikel 6.3 AVG, is het aangewezen te voorzien in (maximale) bewaartermijnen van de te verwerken persoonsgegevens, rekening houdend met het doeleinde en categorieën van gegevens, of toch minstens in de criteria die toelaten deze bewaartermijnen te bepalen.

24. Louter volledigheidshalve vestigt de Autoriteit er de aandacht op dat de vereisten van artikel 5.1.e) AVG geen afbreuk doen aan de voorschriften vervat in de *Archiefwet* van 24 juni 1955.

## **6. Verwerkingsverantwoordelijken**

25. De FOD Justitie is de verstreckende verwerkingsverantwoordelijke (artikel 73, § 2, Burgerlijk Wetboek). Het ontwerp identificeert de FOD Buitenlandse Zaken niet in zoveel woorden als de ontvangende verwerkingsverantwoordelijke, maar de tekst laat daar geen twijfel over bestaan gelet op het feit dat de toegang:

- specifiek aan de FOD Buitenlandse Zaken wordt verleend;
- wordt verleend met het oog op een doeleinde waarmee de FOD Buitenlandse Zaken wettelijk werd belast.

## **7. Beveiliging**

26. Louter volledigheidshalve vestigt de Autoriteit de aandacht op de vereisten van de artikelen 5.1.f) en 32 AVG.

27. Artikel 32 AVG verplicht 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.

28. Artikel 32 AVG wijst in dit verband op een aantal voorbeeldmaatregelen om, waar passend, een op het risico afgestemd beveiligingsniveau te waarborgen:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

29. Voor de concrete uitwerking hiervan wijst de Autoriteit op de Aanbeveling van de Commissie voor de bescherming van de persoonlijke levenssfeer<sup>10</sup> ter voorkoming van gegevenslekken en op het document Referentiemaatregelen<sup>11</sup> inzake beveiliging die bij elke verwerking van persoonsgegevens in acht moeten worden genomen. De Autoriteit onderstreept ook het belang van een behoorlijk gebruikers- en toegangsbeheer<sup>12</sup>.

## **OM DEZE REDENEN,**

### **De Autoriteit**

is van oordeel dat de volgende aanpassingen van het ontwerp zich opdringen:

- een uitdrukkelijke verwijzing opnemen naar de bepalingen die de taak van legalisatie en apostille toevertrouwen aan de FOD Buitenlandse Zaken (punt 15);
- de gegevens tot dewelke toegang wordt verleend, vermelden (punten 17 - 19);
- de betrokkenen identificeren (punten 20 en 21);
- de bewaartermijn preciseren (punt 23)

---

<sup>10</sup> Aanbeveling uit eigen beweging van de Commissie voor de bescherming van de persoonlijke levenssfeer nr. 01/2013 van 21 januari 2013 *betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken* ([https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling\\_01\\_2013\\_0.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2013_0.pdf)).

<sup>11</sup> Referentiemaatregelen van de Commissie voor de bescherming van de persoonlijke levenssfeer voor de beveiliging van elke verwerking van persoonsgegevens, Versie 1.0 ([https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/referentiemaatregelen\\_voor\\_de\\_beveiliging\\_van\\_elke\\_verwerking\\_van\\_persoonsgegevens\\_0.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf)).

<sup>12</sup> Zie ook Aanbeveling van de Commissie voor de bescherming van de persoonlijke levenssfeer nr. 01/2008 van 24 september 2008 *met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector* ([https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling\\_01\\_2008\\_0.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2008_0.pdf)).

Verschiede instanties kunnen hiervoor aangepaste technologische oplossingen bieden (zoals bijvoorbeeld de Kruispuntbank van de Sociale zekerheid).

wijst de aanvrager op het belang van de volgende elementen:

- de naleving van artikel 32 AVG en de verplichting van de verwerkingsverantwoordelijke om de gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens (punten 28 en 29).

(get.) Alexandra Jaspar

Directeur van het Kenniscentrum