Advies nr. 147/2019 van 4 september 2019

Betreft: Ontwerp van koninklijk besluit tot uitvoering van artikel 5, §6, van de wet van 5 mei 2019 houdende diverse bepalingen inzake informatisering van Justitie en modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank (CO-A-2019-156)

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 Minister van Justitie, ontvangen op 22 juli 2019;

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

Brengt op 4 september 2019 het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. De Minister van Justitie verzocht op 22 juli 2019 het advies van de Autoriteit over een ontwerp van koninklijk besluit *tot uitvoering van artikel 5, §6, van de wet van 5 mei 2019 houdende diverse bepalingen inzake informatisering van Justitie en modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank (*hierna "het Ontwerp").

2. Het Ontwerp heeft tot doel om nadere invulling te geven aan de categorieën van gegevens bedoeld in artikel 5, §§1 tot 5 van de wet van 5 mei 2019 *houdende diverse bepalingen inzake informatisering van Justitie en modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank* (hierna "de wet van 5 mei 2019") [1], die verwerkt worden in de gegevensbank "Sidis Suite"[2]. In laatstgenoemde databank worden persoonsgegevens van gedetineerden verwerkt door de Federale Overheidsdienst Justitie en deze overheidsdienst is in artikel 4 van de wet van 5 mei 2019 ook expliciet aangeduid als verwerkingsverantwoordelijke.

3. De gegevenscategorieën die in het Ontwerp nader omschreven worden en die aldus in de Sidis Suite databank zullen opgenomen worden, hebben betrekking op de volgende categorieën van betrokkenen[3]: gedetineerden, kinderen die bij gedetineerden verblijven, bezoekers van gedetineerden[4], andere personen die penitentiaire inrichtingen betreden en slachtoffers van gedetineerden.

II. ONDERZOEK VAN DE ADVIESAANVRAAG

4. **Ten eerste** onderlijnt de Autoriteit voor de goede orde dat het Ontwerp onder de werkingssfeer van de AVG valt en niet – zoals misschien logischerwijze zou kunnen verwacht worden – onder Titel 2 van de WVG[5]. De WVG somt immers op limitatieve wijze de diensten op die onder het toepassingsgebied van de Richtlijn Politie & Justitie[6] vallen en de penitentiaire

---

[1] De Autoriteit en haar rechtsvoorganger, met name de Commissie voor de Bescherming van de Persoonlijke levenssfeer, spraken zich in het verleden meermaals uit over de ontwerpteksten die aan de basis lagen van de wet van 5 mei 2019 (zie adviezen nrs. 10/2017, 50/2017 & 95/2018).

[2] Artikel 5, §6 van de wet van 5 mei 2019 voorziet in een delegatie aan de Koning om deze gegevenscategorieën nader te omschrijven.

[3] Zie artikel 5, §§1 tot 5 van de wet van 5 mei 2019.

[4] *"Bloed- en aanverwanten in de rechte lijn, de voogd, de echtgenoot, de wettelijk of feitelijk samenwonende partner, de broers, zusters, ooms en tantes worden toegelaten tot het bezoek aan de gedetineerden (…)"* (artikel 59 van de Basiswet *betreffende het gevangeniswezen en de rechtspositie van de gedetineerden,* waarnaar artikel 5, §3 van de wet van 5 mei 2019 verwijst).

[5] Zie randnummer 7 van advies nr. 95/2018.

[6] Richtlijn 2016/680/EU van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het*

administratie wordt hier niet in vermeld, waardoor haar verwerkingen **onder de AVG ressorteren**[7].

5. **Ten tweede** brengt de Autoriteit in herinnering dat artikel 22 van de Grondwet de wetgever verbiedt om af te zien van de mogelijkheid om zelf te bepalen welke inmengingen het recht op eerbiediging van de persoonlijke levenssfeer kunnen beknotten[8]. In deze context is een delegatie aan de Koning *"niet in strijd met het wettigheidsbeginsel 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[9]".* De Autoriteit constateert dat artikel 5 van de wet van 5 mei 2019 effectief de essentiële elementen van de gegevenscategorieën bepaalt die in Sidis Suite verwerkt worden en dat de in artikel 5, §6, voorziene delegatie aan de Koning voor de nadere precisering van deze categorieën (wat het voorwerp uitmaakt van het Ontwerp – zie randnummers 1 & 2) aldus **de toets aan het wettigheidsbeginsel doorstaat.**

6. **Ten derde** stelt de Autoriteit vast dat het Ontwerp omschrijft welke gegevens in de Sidis Suite databank zullen opgenomen worden. Voor zover de Autoriteit dit kan beoordelen[10] en onverminderd een aantal punctuele opmerkingen in randnummer 8, heeft zij geen bijzondere opmerkingen over de aard van de gegevenscategorieën die er in worden opgesomd. Zij heeft echter wel een principieel bezwaar tegen het feit dat uit de bewoordingen van het Ontwerp blijkt dat de erin opgesomde gegevens niet exhaustief zijn. De keuze voor niet-limitatieve opsommingen wordt als volgt verklaard: *"(…) om rekening te houden met eventuele vergetelheden en met het onvermijdelijk evolutieve karakter van elke gegevensbank" [11].* De

---

onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[7] Cf. artikel 2.2. punt d), AVG, en de artikelen 25, 26, 7°, & 27 van de WVG.

[8] 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, blz1 21-122.
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.

[9] 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 4482015 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.

[10] De verwerkingsverantwoordelijke – met name de FOD Justitie – is immers het beste geplaatst om te bepalen welke gegevens noodzakelijk zijn om de vooropgestelde doeleinden te bereiken.

[11] P. 2 van het Verslag aan de Koning bij het Ontwerp.

Autoriteit deelt dit standpunt niet en onderlijnt dat **het juist de bedoeling van het Ontwerp zou moeten zijn om tot een transparante, exhaustieve opsomming te komen van alle gegevens die in Sidis Suite verwerkt worden.** Een niet-limitatieve opsomming strookt niet met de dataprotectie-principes[12] en maakt het ook onmogelijk om een volledige proportionaliteitstoets in de zin van artikel 5.1.c) AVG uit te voeren. Het feit dat de Sidis Suite-gegevensbank onvermijdelijk zal evolueren in de tijd dient aldus opgevangen te worden door de inhoud van het uitvoeringsbesluit waarin de gegevenscategorieën nader worden gespecificeerd ook mee te laten evolueren.

7. Hierbij aansluitend merkt de Autoriteit eveneens op dat het Ontwerp slechts uitvoering geeft aan artikel 5, §6, van de wet van 5 mei 2019, terwijl deze wet ook in andere delegaties aan de uitvoerende macht voorziet waarvan de concrete invulling een significante impact op de proportionaliteit van de beoogde verwerkingen zal hebben[13]. Zij adviseert dan ook om het Ontwerp parallel met die andere uitvoeringsbesluiten op te stellen, ten einde een allesomvattende proportionaliteitstoets te kunnen uitvoeren.

8. **Ten vierde** heeft de Autoriteit een aantal punctuele bemerkingen bij de volgende noties die in het Ontwerp gehanteerd worden:

- De termen "identificatienummer van de sociale zekerheid" en "bisnummer" worden in meerdere artikels vermeld en de Autoriteit adviseert om deze in lijn te brengen met de formulering die in artikel 8 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* gebruikt wordt.
- Het is niet duidelijk wat met de notie "individueel detentieplan"[14] bedoeld wordt. In de mate dat deze term niet in andere regelgeving gedefinieerd zou worden, verzoekt de Autoriteit om hiervoor in het Ontwerp in een definitie te voorzien.

9. **Ten vijfde** wijst de Autoriteit op artikel 32 AVG, dat de verwerkingsverantwoordelijke verplicht is 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

[12] Zie artikel 6.3 van de AVG, samengelezen met de artikelen 22 van de Grondwet en 8 van het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden.

[13] Artikel 7, §2, van de wet van 5 mei 2019 voorziet bijvoorbeeld nog in een delegatie aan de Koning om de doeleinden te bepalen waarvoor de organisaties die in artikel 7, §1, van deze wet worden opgesomd hun leesrecht in Sidis Suite mogen uitoefenen. En artikel 9 van de wet van 5 mei 2019 stipuleert dat de Koning nadere regels dient uit te vaardigen betreffende de periode gedurende dewelke gegevens in Sidis Suite beschikbaar en raadpleegbaar dienen te zijn. Vooral de inhoud van het eerstgenoemde uitvoeringsbesluit is belangrijk om een proportionaliteitstoets te kunnen uitvoeren betreffende de gegevens die ingevolge het Ontwerp in Sidis Suite zullen verwerkt worden.

[14] Artikel 2, §3, 3°, van het Ontwerp.

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.

10. 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.

11. Voor de concrete uitwerking hiervan wijst de Autoriteit op de Aanbeveling van de Commissie voor de bescherming van de persoonlijke levenssfeer[15] ter voorkoming van gegevenslekken en op het document "Referentiemaatregelen[16] 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"[17].

12. Bijzondere categorieën van persoonsgegevens in de zin van de artikelen 9 & 10 AVG behoeven strengere beveiligingsmaatregelen. De artikelen 9 & 10, §2, van de WVG geven aan welke bijkomende veiligheidsmaatregelen minstens zullen moeten worden voorzien:

- de categorieën van personen aanwijzen die de persoonsgegevens kunnen raadplegen, waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;

---

[15] 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).

[16] 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).

[17] 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).
Verschillende instanties kunnen hiervoor aangepaste technologische oplossingen bieden (zoals bijvoorbeeld de Kruispuntbank van de Sociale zekerheid).

- de lijst van de aldus aangewezen categorieën van personen ter beschikking houden van de Autoriteit;
- ervoor zorgen dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling, ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

OM DEZE REDENEN

oordeelt de Autoriteit dat de volgende aanpassingen aan het Ontwerp zich opdringen:

- Op limitatieve wijze de categorieën van de verwerkte persoonsgegevens vastleggen (randnummers 6-7);
- De noties "identificatienummer van de sociale zekerheid", "bisnummer" en "individueel detentieplan" aanpassen/definiëren zoals uitgelegd in randnummer 8.

wijst de Autoriteit 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 (randnummers).

(get.) Alexandra Jaspar
Directeur van het Kenniscentrum