Advies nr 10/2017 van 22 februari 2017

Betreft: wetsvoorstel betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Justitie in het kader van de uitvoering van vrijheidsstraffen en vrijheidsbenemende maatregelen en van het beheer van de inrichtingen waar deze uitvoering plaatsvindt (CO-A-2017-001)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Siegfried Bracke, Voorzitter van de Kamer van Volksvertegenwoordigers ontvangen op 03/01/2017;

Gelet op het verslag van de heer Gert Vermeulen;

Brengt op 22 februari 2017 het volgend advies uit:

VOORAFGAANDE OPMERKING

De Commissie vestigt er de aandacht op dat er recent nieuwe Europese regelgeving inzake de bescherming van persoonsgegevens werd uitgevaardigd: de algemene Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en de Richtlijn voor Politie en Justitie. Deze teksten verschenen in het Europese Publicatieblad van 4 mei 2016[1].

De verordening, meestal GDPR (general data protection regulation) genaamd, is van kracht geworden twintig dagen na publicatie, nl. op 24 mei 2016 en wordt, twee jaar later, automatisch van toepassing: 25 mei 2018. De Richtlijn voor politie en justitie moet via nationale wetgeving omgezet worden tegen uiterlijk 6 mei 2018.

Voor de Verordening betekent dit dat vanaf 24 mei 2016, en gedurende de termijn van twee jaar voor de tenuitvoerlegging, op de lidstaten enerzijds een positieve verplichting rust om alle nodige uitvoeringsbepalingen te nemen en anderzijds ook een negatieve verplichting, de zogenaamde “onthoudingsplicht”. Laatstgenoemde plicht houdt in dat er geen nationale wetgeving mag worden uitgevaardigd die het door de Verordening beoogde resultaat ernstig in gevaar zou brengen. Ook voor de Richtlijn gelden gelijkaardige principes.

Het verdient dan ook aanbeveling om desgevallend nu reeds op deze teksten te anticiperen. En het is in de eerste plaats aan de adviesaanvrager(s) om hier rekening mee te houden in zijn (hun) voorstellen of ontwerpen. De Commissie heeft in onderhavig advies, in de mate van het mogelijke en onder voorbehoud van mogelijke bijkomende toekomstige standpunten, alvast gewaakt over de hoger geschetste negatieve verplichting.

---

[1] 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 (algemene verordening gegevensbescherming)

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

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC)

I. VOORWERP EN CONTEXT VAN DE AANVRAAG

1. Op 3 januari 2017 ontving de Commissie een adviesaanvraag omtrent het wetsvoorstel *betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Justitie in het kader van de uitvoering van vrijheidsstraffen en vrijheidsbenemende maatregelen en van het beheer van de inrichtingen waar deze uitvoering plaatsvindt* (hierna: "het voorstel").

2. Het voorstel handelt over de verwerking van persoonsgegevens van gedetineerden door het Directoraat-generaal Penitentiaire Inrichtingen (hierna: "de penitentiaire administratie") in een speciaal daartoe opgerichte databank, "Sidis Suite" genaamd. De penitentiaire administratie heeft als directoraat-generaal van de FOD Justitie immers de opdracht om uitvoering te verlenen aan de vrijheidsberovende straffen en maatregelen en om de strafinrichtingen te beheren. Om deze opdrachten te kunnen uitvoeren moet de penitentiaire administratie persoonsgegevens verwerken met betrekking tot gedetineerden.

3. De Commissie liet zich in het verleden kritisch uit omtrent het feit dat de verwerkingen in de Sidis Suite-databank niet wetgevend omkaderd zijn[1]. Het Sectoraal Comité voor de Federale Overheid deelde deze kritiek en stond er in een recente beslissing op dat deze databank binnen het jaar effectief wettelijk zou omkaderd worden[2].

4. Het voorstel heeft nu kennelijk tot doel om een antwoord te bieden op deze opmerkingen en om aldus de verwerkingen van persoonsgegevens binnen de Sidis Suite databank in overeenstemming te brengen met de WVP en met artikel 22 van de Grondwet.

II. TEN GRONDE

A. Algemeen standpunt van de Commissie

5. De gegevensverwerkingen in het kader van de Sidis Suite-databank vormen– gelet op de aard en de hoeveelheid verwerkte gegevens, de context en de vooropgestelde doeleinden – een belangrijke

---

[1] Bij schrijven van 15/02/2013 maande de Commissie de penitentiaire administratie aan om een wettelijke basis voor deze gegevensbank voor te bereiden.

Medio 2015 werd er met het oog op een overleg tussen penitentiaire administratie en het secretariaat van de Commissie ook een eerste ontwerptekst besproken.

In haar advies nr. 08/2016 van 24 februari 2016 kon de Commissie niet anders dan vaststellen dat er toen nog steeds geen wettelijke basis was uitgewerkt.

[2] Zie beschikkende gedeelte van beraadslaging FO nr. 39/2016.

inmenging in het privéleven van de betrokkenen. De Commissie heeft daarom steeds het standpunt verdedigd dat deze verwerkingen moeten gedekt zijn door een specifieke wettelijke basis (cf. artikel 22 Grondwet).

6. Het voorstel heeft de verdienste dat het de volgende essentiële elementen van de gegevensverwerkingen binnen Sidis suite probeert vast te leggen:

a. De finaliteiten (artikel 3);
b. De verantwoordelijke voor de verwerking (artikel 4);
c. De categorieën van persoonsgegevens die verwerkt worden (artikel 5);
d. De toegangs –en schrijfrechten binnen Sidis Suite (artikelen 6, 7 en 8) en de geheimhoudingsplicht in hoofde van de personen die over die rechten beschikken (artikel 9);
e. De bewaartermijn (artikelen 10 en 11);
f. De rechten van de betrokkenen (artikel 13).

7. Onverminderd een aantal punctuele opmerkingen (zie hieronder punt B), **staat de Commissie dan ook in beginsel positief ten aanzien van het voorstel**. Zij is er van overtuigd dat het een degelijke vertrekbasis vormt om een antwoord te kunnen bieden op de kritiek die zij in het verleden heeft geuit.

B. Punctuele opmerkingen op het voorstel

a. Artikel 4

8. De FOD Justitie wordt in het voorstel als “verantwoordelijke voor de verwerking” van Sidis Suite aangeduid en de penitentiaire administratie als “beheerder”. De Commissie stelt zich vragen bij de meerwaarde om de “penitentiaire administratie”, die reeds een specifieke definitie krijgt in het voorstel (artikel 2, 4°), ook het etiket “beheerder” te geven. Het komt er immers *de facto* op neer dat DG Penitentiaire Inrichtingen twee verschillende benamingen krijgt in het voorstel: “penitentiaire administratie” en “beheerder”, zonder dat er hiervoor een duidelijke reden is.

9. De term “beheerder” lijkt te zijn ontleend aan artikel 44/11/3bis van de Wet op het Politieambt (hierna “WPA”). Omtrent het voorontwerp van wet *inzake aanvullende maatregelen ter bestrijding van terrorisme*, dat aan de oorsprong ligt van dit artikel 44/11/3bis WPA, verleende de Commissie haar advies nr. 57/2015 van 16 december 2015. In dit voorontwerp van wet stond de oprichting van

"gemeenschappelijke gegevensbanken"[3] centraal en in die gemeenschappelijke gegevensbanken zou informatie verzameld worden over iedere "Foreign Terrorist Fighter" en dit op grond van informatie die zou worden aangeleverd door verschillende bevoegde diensten. De Ministers van Justitie en van Binnenlandse Zaken zouden als de verantwoordelijken voor de verwerking aangeduid worden, aangezien zij vanuit juridisch oogpunt de eindverantwoordelijkheid zouden dragen. Aangezien die gegevensbanken verwerkingen zouden impliceren waarbij meerdere actoren van de strafrechtelijke-, politionele –en veiligheidsketen betrokken zijn, pleitte de Commissie er voor om niet alleen algemene verantwoordelijken voor de verwerking aan te duiden, maar om ook op het niveau van de operationele actoren bepaalde verantwoordelijkheden vast te leggen en dit in het bijzonder om te vermijden dat de kwaliteit van de gegevens snel achteruit zou gaan en om er over te waken dat de controle-instanties (Commissie, COC, Comités P en I) steeds een echt aanspreekpunt op het terrein zouden hebben[4].

10. Door de recente invoeging van artikel 44/11/3bis in de WPA werden voornoemde "gemeenschappelijke gegevensbanken" intussen ook juridisch ingebed, en in §9 van dit artikel wordt ook effectief bepaald dat per databank een "beheerder" moet aangeduid worden en er wordt eveneens vastgelegd welke taken deze beheerders hebben.

11. In Sidis Suite is de situatie enigszins vergelijkbaar met de "gemeenschappelijke gegevensbanken" die hierboven geschetst worden, omdat dit systeem ook zal gevoed en geraadpleegd worden door een hele rist aan diensten. De opdeling in artikel 4 van het voorstel is echter weinig zinvol omdat de penitentiaire administratie bijna op een even hoog en algemeen niveau verantwoordelijk is voor de verwerkingen binnen Sidis Suite, als de FOD Justitie. De penitentiaire administratie als "beheerder" kwalificeren heeft *in casu* dus geen toegevoegde waarde en dreigt integendeel verwarring te creëren.

12. Bovendien lijken niet de FOD Justitie en de penitentiaire administratie de eindverantwoordelijkheden voor de gegevensverwerkingen binnen Sidis suite te dragen, maar lijkt dit daarentegen de rol te zijn van de Minister van Justitie.

13. Daarom suggereert de Commissie om in het voorstel de rol van "verantwoordelijke voor de verwerking" toe te bedelen aan de Minister van Justitie, in plaats van de huidige opdeling tussen de FOD Justitie als verantwoordelijke en de penitentiaire administratie als beheerder[5].

---

[3] Het concept "gemeenschappelijke gegevensbank" is intussen ingebed en uitgewerkt in artikel 44/11/3bis van de Wet op het Politieambt.

[4] Cf. Randnummers 51 en 52 van het advies nr. 57/2015 van 16 december 2015.

[5] Dit impliceert niet alleen een aanpassing van artikel 4 van het voorstel, maar ook van alle andere artikels in het voorstel waarin het concept "beheerder" wordt gebruikt.

14. Het idee van de aanduiding van "beheerders" zou volgens de Commissie desgevallend nog een meerwaarde kunnen hebben, indien het mogelijk zou zijn om binnen het geheel van gegevensuitwisselingen in het kader van Sidis Suite aan een aantal operationele actoren specifieke dataprotectie-verantwoordelijkheden toe te bedelen, op voorwaarde dat de rol van deze actoren dan ook duidelijk gedefinieerd zou worden in het voorstel en dat deze aanpak geen afbreuk zou doen aan de eindverantwoordelijkheid van de echte verantwoordelijke voor de verwerking.

b. Artikel 5

15. In artikel 5 van het voorstel worden de categorieën van gegevens opgesomd die in Sidis Suite verwerkt worden en hierbij worden ook persoonsgegevens betreffende de gezondheid vermeld. De Commissie vestigt er volledigheidshalve de aandacht op dat deze categorie van persoonsgegevens enkel onder de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg mogen verwerkt worden (artikel 7, §4, WVP).

c. Artikel 6

16. Voor de interne gebruikers zal aldus de Memorie van Toelichting bij artikel 6 gebruik gemaakt worden van een systeem van "Identity Management", *"dat de toegang tot de dossiers, gegevens en informatie in Sidis Suite strikt beperkt tot de gemachtigde personen en tot de gegevens die zij nodig hebben voor de uitoefening van hun taken."* De Commissie stelt aldus vast dat het de bedoeling is om (ongetwijfeld complexe) systemen van gedifferentieerde toegang naargelang de "need to know" te installeren en zij onthaalt dit positief[6]. Zij wijst in dit verband ook op de noodzaak om een performant toegang –en gebruikersbeheer uit te bouwen en op de richtlijnen die zij in haar aanbeveling nr. 01/2008 van 24 september 2008 uitgevaardigd heeft.

17. Verder stelt de Commissie vast dat het in artikel 6 voorziene "toegangsrecht" soms blijkbaar ook een "schrijfrecht" impliceert, aangezien in de memorie van toelichting het volgende gesteld wordt: *"Binnen dit systeem van "Identity Management" wordt ook traditioneel het onderscheid gemaakt tussen personen die – in functie van de hen toegekende rol – beheersbevoegdheden hebben (gegevens invoeren, wijzigen) en deze die slechts een consultatiebevoegdheid hebben".*

[6] Volledigheidshalve waarschuwt de Commissie er wel voor dat er in de memorie van toelichting bij artikel 6 mogelijks een te grote restrictie betreffende het toegangsrecht tot gezondheidsgegevens wordt vastgelegd: *"(…) de toegang tot de medische dossiers van de gedetineerden is uiteraard beperkt tot de persoon met de hoedanigheid van beroepsbeoefenaar in de gezondheidszorg."* De Commissie hoopt dat deze restrictie bv. niet in die zin gelezen wordt dat het personeel van penitentiaire inrichtingen helemaal niet in kennis kunnen gesteld worden van gezondheidsgegevens betreffende gedetineerden die belangrijk kunnen zijn voor de veiligheid van het personeel (bv: gedetineerde die HIV heeft). Net voor alle andere persoonsgegevens, moet dus ook voor gezondheidsgegevens een "alles of niets-benadering" vermeden worden en is de strikte toepassing van het *"need to know"*-principe noodzakelijk.

18. Het is evident dat bv. personeelsleden van de penitentiaire administratie ook bepaalde schrijfrechten hebben in Sidis Suite, maar dit blijkt niet uit de huidige bewoordingen van artikel 6 van het voorstel. Ten einde een transparante, duidelijke en sluitende regeling uit te bouwen, verzoekt de Commissie om expliciet in artikel 6 te vermelden dat er aan de interne gebruikers zowel lees –als schrijfrechten kunnen toegekend worden.

d. Artikel 7

19. In artikel 7 van het voorstel worden de overheden, organen en diensten opgesomd die een "geheel of gedeeltelijk recht op toegang" [7] hebben tot Sidis Suite. Het betreft enerzijds de evidente partners in de strafrechts –en veiligheidsketen (politie, parket,…), maar anderzijds ook diensten die op de één of andere manier meewerken aan de strafuitvoering of die nood hebben aan de in Sidis Suite verwerkte informatie om hun wettelijke opdrachten te kunnen uitvoeren.

20. De Commissie merkt vooreerst op dat deze bepaling weliswaar een heldere opsomming biedt van de diensten die geviseerd worden, maar dat in artikel 7 zelf op geen enkele manier wordt afgebakend voor welke doeleinden zij deze gegevens mogen gebruiken. De Commissie verzoekt bijgevolg om te verduidelijken dat al deze diensten de gegevens enkel mogen aanwenden in de mate dat dit noodzakelijk is voor de uitvoering van hun wettelijke opdrachten en om in het uitvoeringsbesluit[8] per dienst te preciseren voor welke specifieke finaliteiten zij de gegevens kunnen aanwenden. Ook het "need to know principe"[9] zou een weerslag moeten krijgen in de tekst van artikel 7. Dit zijn overigens ook twee elementen die zwaar doorwegen in de evaluatie of het voor die diensten al dan niet aangewezen is om in een vrijstelling op de machtigingsplicht te voorzien (cf. infra randnummers 34 e.v.).

21. Ten tweede suggereert de Commissie om duidelijk te vermelden dat de desbetreffende diensten een "leesrecht" krijgen in plaats van een "toegangsrecht", omdat deze woordkeuze nauwkeuriger is.

22. Ten derde is de Commissie van oordeel dat er een discrepantie bestaat tussen de tekst van artikel 7 en de Memorie van toelichting bij dit artikel, met name omdat aan de term "toegangsrecht" een interpretatie wordt gegeven die op privacy-vlak een stuk intrusiever is dan wat in de gangbare betekenis onder deze notie wordt begrepen. Volgens de Memorie moet het "toegangsrecht" dat in

[7] In artikel 7 wordt de term "recht op toegang" gebruikt, terwijl dit wellicht "toegangsrecht" zou moeten zijn. De notie "recht op toegang" wordt in de gangbare betekenis immers gebruikt in de context van artikel 10 WVP en dit artikel 10 WVP staat evident los van wat in artikel 7 van het voorstel wordt beoogd.

[8] Cf. artikel 7, voorlaatste lid, van het voorstel.

[9] De toegang tot de dossiers, gegevens en informatie in Sidis Suite dient strikt beperkt te blijven tot de gemachtigde personen en tot de gegevens die zij nodig hebben voor de uitoefening van hun taken.

artikel 7 verleend wordt immers gezien worden als een *"generiek begrip dat de verschillende gradaties van toegang omvat (met name de zgn. "pull" van gegevens onder de vorm van een rechtstreekste toegang via een geautomatiseerde verbinding met Sidis Suite of, minder verregaand, onder de vorm van een rechtstreekse bevraging (hit/no-hit) van Sidis Suite, als de zgn. "Push" van gegevens onder de vorm van een geautomatiseerde doorzending van gegevens)".*

23. De Commissie heeft ernstige bedenkingen bij deze aanpak, aangezien dit geen transparante regeling is. Zij pleit er daarentegen voor om in het uitvoeringsbesluit bij artikel 7 (en niet enkel in het algemeen in de memorie van toelichting) duidelijk per dienst aan te geven over welk soort "leesrecht" deze dienst beschikt.

24. Ten vierde staat de Commissie positief ten aanzien van de idee om bij de organisatie van het leesrecht van de in artikel 7 bedoelde diensten, maximaal gebruik te maken van de technieken die door dienstenintegratoren kunnen ter beschikking gesteld worden (zie Memorie van Toelichting bij artikel 7). Aangezien de tussenkomst van deze integratoren garanties biedt op het vlak van de degelijke beveiliging van de gegevens, pleit de Commissie er voor om dit principe ook in de tekst van artikel 7 op te nemen.

25. Ten vijfde wenst de Commissie haar bezorgdheid te uiten omtrent de volgende passage uit de Memorie van Toelichting bij artikel 7: *"Om die reden wordt de loutere mededeling van gegevens vanuit Sidis Suite hier niet geviseerd. De penitentiaire administratie deelt enkel gegevens mee aan derde overheden, organen of diensten die daarvoor in hun "eigen" wetgeving over een wettelijke grondslag beschikken. (…)"*

26. Deze paragraaf geeft heel sterk de indruk dat er in de praktijk ook nog andere diensten leesrechten zullen krijgen in Sidis Suite, dan de diensten opgesomd in artikel 7 en de diensten die zullen vermeld worden in het uitvoeringsbesluit dat in de voorlaatste alinea van artikel 7 wordt voorzien. De Commissie onderlijnt dat het juist de bedoeling van het voorstel en het bijhorende uitvoeringsbesluit zou moeten zijn om tot een transparante, exhaustieve opsomming te komen van alle diensten die leesrechten hebben in Sidis Suite. Zij dringt er dan ook sterk op aan om de uit de Memorie geciteerde passage te schrappen en om in artikel 7 (en/of in het uitvoeringsbesluit) in een volledige opsomming te voorzien.

e. <u>Artikel 8</u>

27. In artikel 8 van het voorstel wordt het schrijfrecht in Sidis Suite van de Dienst Vreemdelingenzaken en van de Staatsveiligheid geregeld, aangezien dit beide belangrijke partners zijn van de penitentiaire administratie bij de strafuitvoering.

28. De Commissie merkt dienaangaande op dat in de tekst van artikel 8 de notie “registreert” wordt gebruikt, terwijl de omschrijving “heeft een schrijfrecht” duidelijker en nauwkeuriger zou zijn.

29. Verder gaat de Commissie er van uit dat de lijst van medewerkers van die twee instanties, die toegang zullen hebben tot Sidis Suite, niet alleen *“ter beschikking wordt gehouden”* van de penitentiaire administratie (artikel 8, §§1 & 2, in fine, van het voorstel), maar dat laatstgenoemde deze lijst ook effectief gebruikt in het kader van het gebruikers –en toegangsbeheer tot Sidis Suite (met name om het aspect “hoedanigheid” te kunnen controleren).

f. Artikel 10

30. Artikel 10 van het voorstel bepaalt dat elke in Sidis Suite uitgevoerde verwerking automatisch geregistreerd wordt en dit zowel voor de interne als voor de externe gebruikers. De Commissie meent dat een dergelijke logging in onderhavig geval inderdaad onontbeerlijk is en zij onderschrijft deze bepaling dan ook volledig.

g. Artikel 13

31. Artikel 13 van het voorstel voorziet in een afwijking op bepaalde rechten van de betrokkenen die in de WVP worden voorzien. Hoewel de Commissie hier gelet op de context geen principiële bezwaren tegen heeft, stelt zij zich vragen bij de wijze waarop deze bepaling geformuleerd is.

32. Ten eerste is het mogelijks aangewezen dat de uitzondering niet beperkt wordt tot gegevensverwerkingen die door de penitentiaire administratie worden verricht, maar dat deze voor alle verwerkingen in het kader van Sidis Suite dient te gelden. Wat bijvoorbeeld met de gegevens die door de Dienst Vreemdelingzaken zullen aangeleverd worden (artikel 8 voorstel)? Kan de betrokkene hieromtrent vrij zijn recht van toegang uitoefenen binnen Sidis Suite? De Commissie nodigt de stellers van het ontwerp uit om deze oefening te maken voor alle verwerkingen binnen Sidis Suite die niet door de penitentiaire administratie verricht worden, om zeker te zijn dat het uitzonderingsregime desgewenst alles afdekt.

33. Ten tweede lijkt het volgens de Memorie van toelichting de bedoeling om de uitzonderingsregeling (gedeeltelijk) te beperken tot enkel de gevallen waarin de toepassing van de bestaande WVP-rechten:

a. zou leiden tot kennisname van die gegevens die in Sidis Suite gebruikt worden tot vaststelling van het risicoprofiel van de gedetineerde;

b. een kennisname in hoofde van betrokkene zou impliceren die de veiligheid ernstig in gevaar zou brengen.

Indien dit effectief de bedoeling is van de stellers van het ontwerp, dienen de woorden "In het bijzonder" in het begin van het tweede lid van artikel 13, wellicht te worden geschrapt. De Commissie nodigt de stellers van het ontwerp dan ook uit om artikel 13 op dit punt opnieuw te analyseren.

C. Slotbemerking – Sidis Suite en het machtigingssysteem

34. Artikel 36*bis* WVP schrijft voor dat de elektronische mededelingen van persoonsgegevens door een federale instelling, zoals de penitentiaire administratie, een machtiging vereisen van het Sectoraal comité van de Federale Overheid[10]. Dit artikel laat tegelijk de mogelijkheid om bij Koninklijk besluit uitzonderingen te voorzien op deze machtigingsplicht.

35. Hoewel de Commissie steeds de meerwaarde van het machtigingssysteem benadrukt heeft en nog steeds benadrukt, is zij van oordeel dat in dit specifieke geval in het uitvoeringsbesluit een uitzondering zou kunnen voorzien worden op de voorafgaande machtigingsplicht en dit voor sommige diensten die over leesrechten beschikken in Sidis Suite (zie opsomming in artikel 7 van het voorstel). Het voorstel strekt er immers toe om in een degelijke wettelijke grondslag en omkadering te voorzien om aan deze diensten leesrechten te verlenen in Sidis Suite en die grondslag zal bovendien nog voor een stuk nader worden uitgewerkt in het uitvoeringsbesluit, dat eveneens ter advies van de Commissie zal voorgelegd worden[11].

36. In de hypothese dat deze leesrechten ook effectief voldoende worden gepreciseerd in het uitvoeringsbesluit (zie in het bijzonder de hoger gemaakte opmerkingen in de randnummers 20 en 23), meent de Commissie dat het voor sommige van deze diensten gerechtvaardigd kan zijn om in een uitzondering te voorzien op de machtigingsplicht, aangezien de verwerkingsmodaliteiten dan in belangrijke mate reeds door de regelgeving zouden bepaald worden. De Commissie adviseert om bij de voorbereiding van het uitvoeringsbesluit ten gronde over dit vraagstuk te reflecteren en zij zal dit aspect evident ook evalueren op het ogenblik dat het uitvoeringsbesluit haar ter advies wordt voorgelegd.

---

[10] In de mate dat gezondheidsgegevens toegankelijk worden gesteld is in toepassing van artikel 43, § 2, 3°, van de wet van 13 december 2006 *houdende diverse bepalingen,* een machtiging van het Sectoraal comité van de Sociale Zekerheid en van de Gezondheid vereist.

[11] Artikel 7, voorlaatste lid, van het voorstel.

OM DEZE REDENEN

de Commissie

verleent een gunstig advies, op voorwaarde dat rekening wordt gehouden met de volgende opmerkingen:

- Heldere aanduiding van de verantwoordelijke voor de verwerking (randnummer 13);
- Meer nauwkeurige formulering betreffende de lees –en schrijfrechten in de artikelen 6 en 8 (randnummers 17, 18 en 28)
- Betere uitwerking van de leesrechten in artikel 7 en dit conform de vijf opmerkingen gemaakt in de randnummers 19 t.e.m. 26;
- Meer nauwkeurige formulering van de beperkingen op de rechten van de betrokkenen (randnummers 32 en 33);
- In het uitvoeringsbesluit desgevallend uitzonderingen voorzien op de machtigingsplicht (randnummer 36).

De Wnd. Administrateur, De Voorzitter,

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