DOC 54 **2194/003**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

28 februari 2017

# 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**

**ADVIES VAN DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER NR. 10/2017 VAN 22 FEBRUARI 2017**

*Zie:*

Doc 54 **2194/ (2016/2017):**
001: Wetsvoorstel van de heer Terwingen, mevrouw Becq en de heren Foret en Goffin.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

28 février 2017

# PROPOSITION DE LOI

**concernant le traitement de données à caractère personnel par le Service public fédéral Justice dans le cadre de l'exécution des peines et des mesures privatives de liberté et de la gestion des établissements dans lesquels cette exécution s'effectue**

**AVIS DE LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE N° 10/2017 DU 22 FÉVRIER 2017**

*Voir:*

Doc 54 **2194/ (2016/2017):**
001: Proposition de loi de M. Terwingen, Mme Becq et MM. Foret et Goffin.

| | | |
|---|---|---|
| *N-VA* | : | *Nieuw-Vlaamse Alliantie* |
| *PS* | : | *Parti Socialiste* |
| *MR* | : | *Mouvement Réformateur* |
| *CD&V* | : | *Christen-Democratisch en Vlaams* |
| *Open Vld* | : | *Open Vlaamse liberalen en democraten* |
| *sp.a* | : | *socialistische partij anders* |
| *Ecolo-Groen* | : | *Ecologistes Confédérés pour l'organisation de luttes originales – Groen* |
| *cdH* | : | *centre démocrate Humaniste* |
| *VB* | : | *Vlaams Belang* |
| *PTB-GO!* | : | *Parti du Travail de Belgique – Gauche d'Ouverture* |
| *DéFI* | : | *Démocrate Fédéraliste Indépendant* |
| *PP* | : | *Parti Populaire* |
| *Vuye&Wouters* | : | *Vuye&Wouters* |

*Afkortingen bij de nummering van de publicaties:*

| | |
|---|---|
| *DOC 54 0000/000:* | *Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer* |
| *QRVA:* | *Schriftelijke Vragen en Antwoorden* |
| *CRIV:* | *Voorlopige versie van het Integraal Verslag* |
| *CRABV:* | *Beknopt Verslag* |
| *CRIV:* | *Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)* |
| *PLEN:* | *Plenum* |
| *COM:* | *Commissievergadering* |
| *MOT:* | *Moties tot besluit van interpellaties (beigekleurig papier)* |

*Abréviations dans la numérotation des publications:*

| | |
|---|---|
| *DOC 54 0000/000:* | *Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif* |
| *QRVA:* | *Questions et Réponses écrites* |
| *CRIV:* | *Version Provisoire du Compte Rendu intégral* |
| *CRABV:* | *Compte Rendu Analytique* |
| *CRIV:* | *Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)* |
| *PLEN:* | *Séance plénière* |
| *COM:* | *Réunion de commission* |
| *MOT:* | *Motions déposées en conclusion d'interpellations (papier beige)* |

*Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers*

*Bestellingen:*
*Natieplein 2*
*1008 Brussel*
*Tel. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.dekamer.be*
*e-mail : publicaties@dekamer.be*

*De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier*

*Publications officielles éditées par la Chambre des représentants*

*Commandes:*
*Place de la Nation 2*
*1008 Bruxelles*
*Tél. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.lachambre.be*
*courriel : publications@lachambre.be*

*Les publications sont imprimées exclusivement sur du papier certifié FSC*


**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,

An Machtens

De Voorzitter,

Willem Debeuckelaere

**Avis n° 10/2017 du 22 février 2017**

**Objet :** proposition de loi concernant le traitement de données à caractère personnel par le Service public fédéral Justice dans le cadre de l'exécution des peines et des mesures privatives de liberté et de la gestion des établissements dans lesquels cette exécution s'effectue (CO-A-2017-001)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis de Monsieur Siegfried Bracke, Président de la Chambre des Représentants, reçue le 03/01/2017 ;

Vu le rapport de Monsieur Gert Vermeulen ;

Émet, le 22 février 2017 l'avis suivant :

**REMARQUE PRÉALABLE**

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation ou RGPD pour Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

## I. OBJET ET CONTEXTE DE LA DEMANDE

1. Le 3 janvier 2017, la Commission a reçu une demande d'avis au sujet de la proposition de loi *concernant le traitement de données à caractère personnel par le Service public fédéral Justice dans*

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Directive (UE) du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

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

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

*le cadre de l'exécution des peines et des mesures privatives de liberté et de la gestion des établissements dans lesquels cette exécution s'effectue* (ci-après : "la proposition").

2. La proposition concerne le traitement de données à caractère personnel de détenus par la direction générale des Établissements pénitentiaires (ci-après : "l'administration pénitentiaire") dans une banque de données créée spécialement à cet effet, appelée "Sidis Suite". En tant que direction générale du SPF Justice, l'administration pénitentiaire a en effet la mission d'exécuter des peines et des mesures privatives de liberté et de gérer des établissements pénitentiaires. Pour pouvoir réaliser ces missions, l'administration pénitentiaire doit traiter des données à caractère personnel concernant les détenus.

3. La Commission a été critique par le passé à l'égard du fait que les traitements dans la banque de données Sidis Suite ne bénéficiaient pas d'un cadre législatif[1]. Le Comité sectoriel pour l'Autorité Fédérale a partagé cette critique et a insisté dans une décision récente pour que cette banque de données soit effectivement encadrée légalement dans l'année[2].

4. À présent, la proposition entend manifestement répondre à ces remarques et faire en sorte que les traitements de données à caractère personnel au sein de la banque de données Sidis Suite soient conformes à la LVP et à l'article 22 de la Constitution.

## II. QUANT AU FOND

### *A. Point de vue général de la Commission*

5. Les traitements de données dans le cadre de la banque de données Sidis Suite constituent – eu égard à la nature et à la quantité des données traitées, au contexte et aux finalités envisagées – une ingérence importante dans la vie privée des personnes concernées. La Commission a dès lors toujours défendu la position selon laquelle ces traitements devaient être couverts par une base légale spécifique (cf. l'article 22 de la Constitution).

6. La proposition a le mérite de tenter de définir les éléments essentiels suivants des traitements de données au sein de Sidis Suite :

---

[1] Par courrier du 15/02/2013, la Commission a sommé l'administration pénitentiaire de préparer une base légale pour cette banque de données.

À la mi-2015, un premier projet de texte a également été discuté en vue d'une concertation entre l'administration pénitentiaire et le Secrétariat de la Commission.

Dans son avis n° 08/2016 du 24 février 2016, la Commission a dû constater qu'aucune base légale n'avait encore été élaborée.

[2] Voir le dispositif de la délibération AF n° 39/2016.

a. les finalités (article 3) ;
b. le responsable du traitement (article 4) ;
c. les catégories de données à caractère personnel qui sont traitées (article 5) ;
d. les droits d'accès et d'écriture au sein de Sidis Suite (articles 6, 7 et 8) et l'obligation de confidentialité dans le chef des personnes qui disposent de ces droits (article 9) ;
e. le délai de conservation (articles 10 et 11) ;
f. les droits des personnes concernées (article 13).

7. Sous réserve de quelques remarques ponctuelles (voir ci-après au point B), **la Commission est donc en principe positive à l'égard de la proposition**. Elle est convaincue qu'elle constitue une base solide susceptible de répondre aux critiques qu'elle avait émises précédemment.

***B. Remarques ponctuelles sur la proposition***

*a. Article 4*

8. Dans la proposition, le SPF Justice est désigné comme "responsable du traitement" de Sidis Suite et l'administration pénitentiaire comme "gestionnaire". La Commission s'interroge sur la plus-value de conférer aussi l'étiquette de "gestionnaire" à l' "administration pénitentiaire", qui fait déjà l'objet d'une définition spécifique dans la proposition (article 2, 4°). En effet, il en résulte *de facto* que la DG des Établissements pénitentiaires se voit attribuer deux dénominations différentes dans la proposition : "administration pénitentiaire" et "gestionnaire", sans raison claire.

9. Le terme "gestionnaire" semble être emprunté à l'article 44/11/3*bis* de la loi *sur la fonction de police* (ci-après la "LFP"). La Commission avait émis l'avis n° 57/2015 du 16 décembre 2015 *concernant l'avant-projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme*, avant-projet qui est à l'origine de cet article 44/11/3*bis* de la LFP. La création de "banques de données communes"[3] occupait une place centrale dans cet avant-projet de loi et c'est dans ces banques de données communes que devaient être collectées des informations sur tout "Foreign Terrorist Fighter" sur la base d'informations fournies par différents services compétents. Les ministres de la Justice et de l'Intérieur devaient être désignés comme responsables du traitement, étant donné que d'un point de vue juridique, ils devaient assumer la responsabilité finale. Étant donné que ces banques de données donneraient lieu à des traitements impliquant plusieurs acteurs de la chaîne pénale, policière et de sécurité, la Commission avait plaidé non seulement pour la désignation de responsables du traitement généraux, mais aussi pour l'établissement de certaines responsabilités au niveau des acteurs opérationnels, et ce en particulier pour éviter que la qualité des données se dégrade

[3] Le concept de "banque de données commune" a entre-temps été intégré et développé à l'article 44/11/3*bis* de la loi *sur la fonction de police*.

rapidement et pour veiller à ce que les instances de contrôle (Commission, COC, Comités P et R) aient toujours un véritable point de contact sur le terrain[4].

10. Le récent ajout de l'article 44/11/3*bis* dans la LFP a entre-temps permis de conférer un ancrage juridique aux "banques de données communes" précitées, et le § 9 de cet article dispose aussi effectivement que par banque de données, un "gestionnaire" doit être désigné et définit également quelles sont les tâches de ces gestionnaires.

11. Dans Sidis Suite, la situation est quelque peu comparable avec les "banques de données communes" dépeintes ci-avant, parce que ce système sera également alimenté et consulté par toute une série de services. La subdivision à l'article 4 de la proposition est toutefois peu judicieuse du fait que l'administration pénitentiaire est déjà responsable, à un niveau quasiment aussi élevé et général, des traitements au sein de Sidis Suite, comme le SPF Justice. Qualifier l'administration pénitentiaire de "gestionnaire" ne présente donc en l'occurrence aucune plus-value et risque au contraire de semer la confusion.

12. En outre, le SPF Justice et l'administration pénitentiaire ne semblent pas porter les responsabilités finales pour les traitements de données au sein de Sidis suite ; cela semble au contraire relever du rôle du Ministre de la Justice.

13. La Commission suggère dès lors que la proposition attribue le rôle de "responsable du traitement" au Ministre de la Justice, en lieu et place de la répartition actuelle entre le SPF Justice en tant que responsable et l'administration pénitentiaire en tant que gestionnaire[5].

14. D'après la Commission, l'idée de la désignation de "gestionnaires" pourrait le cas échéant encore présenter une plus-value s'il était possible, dans l'ensemble des échanges de données dans le cadre de Sidis Suite, de confier des responsabilités spécifiques en matière de protection des données à plusieurs acteurs opérationnels, à condition que le rôle de ces acteurs soit alors clairement défini dans la proposition et que cette approche ne porte pas préjudice à la responsabilité finale du véritable responsable du traitement.

---

[4] Cf. les points 51 et 52 de l'avis n° 57/2015 du 16 décembre 2015.

[5] Cela implique non seulement une adaptation de l'article 4 de la proposition, mais aussi de tous les autres articles de la proposition où l'on évoque le concept de "gestionnaire".

*b. Article 5*

15. L'article 5 de la proposition énumère les catégories de données traitées dans Sidis Suite, énumération dans laquelle on retrouve aussi des données à caractère personnel relatives à la santé. Par souci d'exhaustivité, la Commission attire l'attention sur le fait que cette catégorie de données à caractère personnel ne peut être traitée que sous la responsabilité d'un professionnel des soins de santé (article 7, § 4 de la LVP).

*c. Article 6*

16. Pour les utilisateurs internes, on utilisera, d'après l'Exposé des motifs de l'article 6, un système d' "Identity Management", qui "*part du principe que l'accès aux dossiers, données et informations dans Sidis Suite est strictement limité aux personnes autorisées et aux données nécessaires à l'exercice de leurs tâches.*". La Commission constate donc que l'intention est d'installer des systèmes (assurément complexes) d'accès différencié selon le principe "need to know", ce qu'elle accueille positivement[6]. Elle souligne aussi à cet égard la nécessité d'élaborer une gestion des utilisateurs et des accès performante et rappelle les directives qu'elle a promulguées dans sa recommandation n° 01/2008 du 24 septembre 2008.

17. Par ailleurs, la Commission constate que le "droit d'accès" prévu à l'article 6 implique apparemment aussi parfois un "droit d'écriture", étant donné que l'Exposé des motifs précise ce qui suit : *"Dans ce système d' "identity Management", la distinction traditionnelle [est faite] entre les personnes qui - en fonction du rôle qui leur est attribué - ont des compétences en matière de gestion (introduction, modification de données) et celles qui n'ont qu'une compétence de consultation".*

18. Il est évident que les membres du personnel de l'administration pénitentiaire ont par exemple aussi certains droits d'écriture dans Sidis Suite, mais cela ne ressort pas du libellé actuel de l'article 6 de la proposition. En vue d'un règlement transparent, clair et cohérent, la Commission demande de mentionner explicitement à l'article 6 que des droits tant de lecture que d'écriture peuvent être attribués aux utilisateurs internes.

---

[6] Par souci d'exhaustivité, la Commission avertit toutefois que l'Exposé des motifs de l'article 6 établit probablement une trop grande restriction quant au droit d'accès aux données relatives à la santé : *"(...) l'accès aux dossiers médicaux des détenus est évidemment limité à la personne qui a la qualité de praticien professionnel en matière de soins de santé."* La Commission espère que cette restriction n'est par exemple pas interprétée en ce sens que le personnel d'établissements pénitentiaires ne peut en aucune façon avoir connaissance de données relatives à la santé concernant des détenus qui peuvent être importantes pour la sécurité du personnel (par exemple un détenu qui est porteur du VIH). Tout comme pour les autres données à caractère personnel, il faut donc également éviter pour les données relatives à la santé une "approche tout ou rien" et la stricte application du principe "*need to know*" est nécessaire.

*d. Article 7*

19. L'article 7 de la proposition énumère les autorités, organes et services qui ont un "droit d'accéder intégralement ou partiellement" [7] à Sidis Suite. Il s'agit d'une part des partenaires évidents de la chaîne pénale et de sécurité (police, parquet, ...), mais d'autre part aussi des services qui collaborent d'une manière ou d'une autre à l'exécution des peines ou qui ont besoin des informations traitées dans Sidis Suite pour pouvoir accomplir leurs tâches légales.

20. Premièrement, la Commission fait remarquer que cette disposition comporte certes une énumération claire des services visés, mais qu'à l'article 7 proprement dit, on ne délimite en aucune façon les finalités pour lesquelles ils peuvent utiliser ces données. La Commission demande dès lors de préciser que tous ces services ne peuvent utiliser les données que dans la mesure où cela se révèle nécessaire à l'exécution de leurs tâches légales et de préciser par service dans l'arrêté d'exécution[8] les finalités spécifiques pour lesquelles ils peuvent utiliser ces données. Le principe "need to know"[9] devrait aussi se refléter dans le texte de l'article 7. Il s'agit d'ailleurs aussi de deux éléments qui sont prépondérants dans l'évaluation destinée à savoir s'il est ou non recommandé de prévoir une dispense de l'obligation d'autorisation (cf. infra, points 34 e.s.).

21. Deuxièmement, la Commission suggère de mentionner clairement que les services en question ont un "droit de lecture" au lieu d'un "droit d'accès", ce choix terminologique étant plus précis.

22. Troisièmement, la Commission estime qu'il y a une discordance entre le texte de l'article 7 et l'Exposé des motifs de cet article, notamment eu égard au fait que l'on donne aux termes "droit d'accès" une interprétation qui, en termes de vie privée, est plus intrusive que celle comprise dans la signification usuelle de cette notion. D'après l'Exposé des motifs, le "droit d'accès" qui est octroyé à l'article 7 est en effet vu comme "*une notion générique et englobe les différentes gradations d'accès (à savoir tant le "pull" de données sous la forme d'un accès direct via une connexion automatisée avec Sidis Suite ou, de manière moins étendue, sous la forme d'une interrogation directe de Sidis Suite (hit/no-hit) que le "push" de données sous la forme d'un envoi automatisé de données).*"

23. La Commission émet de sérieuses réserves quant à cette approche, ce règlement n'étant pas transparent. Elle plaide par contre pour que l'on indique clairement par service dans l'arrêté

---

[7] L'article 7 utilise en néerlandais les termes "recht op toegang" (droit d'accès en français), tandis qu'il devrait probablement être question du "toegangsrecht" (également droit d'accès en français). La notion de "recht op toegang" est en effet utilisée dans sa signification courante dans le contexte de l'article 10 de la LVP et cet article 10 de la LVP n'a évidemment pas de lien avec ce que vise l'article 7 de la proposition.

[8] Cf. article 7, avant-dernier alinéa de la proposition.

[9] L'accès aux dossiers, données et informations dans Sidis Suite doit rester strictement limité aux personnes habilitées et aux données dont elles ont besoin pour accomplir leurs tâches.

d'exécution de l'article 7 (et pas uniquement de manière générale dans l'Exposé des motifs) de quel type de "droit de lecture" chaque service dispose.

24. Quatrièmement, la Commission est positive à l'égard de l'idée que pour l'organisation du droit de lecture des services visés à l'article 7, on utilise au maximum les techniques qui peuvent être mises à disposition par des intégrateurs de services (voir l'Exposé des motifs de l'article 7). Étant donné que l'intervention de ces intégrateurs offre des garanties au niveau de la bonne sécurisation des données, la Commission plaide pour que ce principe soit également repris dans le texte de l'article 7.

*25.* Cinquièmement, la Commission souhaite exprimer son inquiétude à l'égard du passage suivant de l'Exposé des motifs de l'article 7 : *"C'est la raison pour laquelle la simple communication de données de Sidis Suite n'est pas visée ici. L'administration pénitentiaire ne communique des données qu'aux autorités tierces ou aux organes ou services tiers qui disposent d'une base légale à cet effet dans leur "propre" législation. (...)"*

26. Ce paragraphe donne fortement l'impression que dans la pratique, d'autres services encore auront des droits de lecture dans Sidis Suite, par rapport à ceux énumérés à l'article 7 et aux services qui seront mentionnés dans l'arrêté d'exécution qui est prévu à l'avant-dernier alinéa de l'article 7. La Commission souligne que ce devrait précisément être l'objectif de la proposition et de l'arrêté d'exécution y afférent de parvenir à une énumération transparente et exhaustive de tous les services qui ont des droits de lecture dans Sidis Suite. Elle insiste dès lors fermement pour que l'on supprime le passage cité dans l'Exposé des motifs et que l'on prévoie une énumération exhaustive à l'article 7 (et/ou dans l'arrêté d'exécution).

*e. Article 8*

27. L'article 8 de la proposition régit le droit d'écriture dans Sidis Suite pour l'Office des étrangers et la Sûreté de l'État, étant donné que ce sont deux partenaires importants de l'administration pénitentiaire dans l'exécution des peines.

28. La Commission fait remarquer à cet égard que dans le texte de l'article 8, on utilise la notion de "enregistrer", tandis que la description "a un droit d'écriture" serait plus claire et précise.

29. Par ailleurs, la Commission part du principe que la liste des collaborateurs de ces deux instances, qui auront accès à Sidis Suite, non seulement "*est tenue à la disposition*" de l'administration pénitentiaire (article 8, §§ 1 & 2, *in fine*, de la proposition), mais que cette dernière utilise aussi effectivement cette liste dans le cadre de la gestion des utilisateurs et des accès de Sidis Suite (notamment pour pouvoir contrôler l'aspect "qualité").

*f. Article 10*

30. L'article 10 de la proposition dispose que chaque traitement effectué dans Sidis Suite est automatiquement enregistré, et ce tant pour les utilisateurs internes qu'externes. La Commission estime qu'une telle journalisation est en effet indispensable en l'espèce et adhère dès lors pleinement à cette disposition.

*g. Article 13*

31. L'article 13 de la proposition prévoit une dérogation à certains droits de la personne concernée prévus dans la LVP. Bien que la Commission n'ait pas de remarque de principe à ce sujet, vu le contexte, elle s'interroge quant à la manière dont cette disposition est formulée.

32. Premièrement, il est peut-être recommandé que l'exception ne soit pas limitée aux traitements de données effectués par l'administration pénitentiaire, mais qu'elle doive s'appliquer à tous les traitements dans le cadre de Sidis Suite. Qu'en est-il par exemple des données qui seront fournies par l'Office des étrangers (article 8 de la proposition) ? La personne concernée peut-elle à cet égard exercer librement son droit d'accès au sein de Sidis Suite ? La Commission invite les auteurs de la proposition à faire cet exercice pour tous les traitements au sein de Sidis Suite qui ne sont pas effectués par l'administration pénitentiaire, afin de s'assurer que le régime d'exception couvre tout ce qu'il doit couvrir.

33. Deuxièmement, il semble d'après l'Exposé des motifs que l'intention soit de limiter (partiellement) le régime d'exception aux seuls cas où l'application des droits existants issus de la LVP :

a. donnerait lieu à la prise de connaissance de ces données qui sont utilisées dans Sidis Suite pour établir le profil de risque du détenu ;
b. impliquerait une prise de connaissance dans le chef de la personne concernée qui compromettrait gravement la sécurité.

Si telle est effectivement l'intention des auteurs de la proposition, les termes "en particulier" au début du deuxième alinéa de l'article 13 doivent peut-être être supprimés. La Commission invite dès lors les auteurs de la proposition à analyser de nouveau l'article 13 sur ce point.

### *C. Remarque finale – Sidis Suite et le système d'autorisation*

34. L'article 36*bis* de la LVP dispose que les communications électroniques de données à caractère personnel par une institution fédérale, comme l'administration pénitentiaire, requièrent une autorisation du Comité sectoriel pour l'Autorité Fédérale[10]. Cet article laisse en même temps la possibilité de prévoir, par arrêté royal, des exceptions à cette obligation d'autorisation.

35. Bien que la Commission ait toujours souligné la plus-value du système d'autorisation et la souligne toujours, elle estime que dans ce cas spécifique, une exception à l'obligation d'autorisation préalable pourrait être prévue dans l'arrêté d'exécution, et ce pour certains services qui disposent de droits de lecture dans Sidis Suite (voir énumération à l'article 7 de la proposition). La proposition vise en effet à prévoir un bon fondement légal et un bon encadrement légal pour octroyer à ces services des droits de lecture dans Sidis Suite et ce fondement sera en outre élaboré davantage dans l'arrêté d'exécution, qui sera également soumis à l'avis de la Commission[11].

36. Dans l'hypothèse où ces droits de lecture sont aussi précisés suffisamment dans l'arrêté d'exécution (voir en particulier les remarques formulées ci-avant aux points 20 et 23), la Commission estime qu'il peut être légitime de prévoir pour certains services une exception à l'obligation d'autorisation, étant donné que les modalités de traitement seraient alors déjà déterminées en grande partie par la réglementation. La Commission recommande de réfléchir à cette question lors de la préparation quant au fond de l'arrêté d'exécution et elle évaluera bien entendu aussi cet aspect au moment où l'arrêté d'exécution lui sera soumis pour avis.

---

[10] Dans la mesure où des données relatives à la santé sont rendues accessibles, une autorisation du Comité sectoriel de la Sécurité sociale et de la Santé est requise, en application de l'article 43, § 2, 3° de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*.

[11] Article 7, avant-dernier alinéa de la proposition.

**PAR CES MOTIFS,**

**la Commission**

**émet** un avis favorable, à condition qu'il soit tenu compte des remarques suivantes :

- désignation claire du responsable du traitement (point 13) ;
- formulation plus précise concernant les droits de lecture et d'écriture aux articles 6 et 8 (points 17, 18 et 28) ;
- meilleur développement des droits de lecture à l'article 7, et ce conformément aux cinq remarques formulées aux points 19 à 26 inclus ;
- formulation plus précise des limitations des droits des personnes concernées (points 32 et 33) ;
- prévoir le cas échéant des exceptions à l'obligation d'autorisation dans l'arrêté d'exécution (point 36).

L'Administrateur f.f., Le Président,

An Machtens Willem Debeuckelaere

CBPL
**Commissie** voor de **bescherming** van de **persoonlijke levenssfeer**

**Dossier behandeld door :** Allemeersch Koenraad
**T:** + 32 (0)2 274 48 43
**F:** + 32 (0)2 274 48 35
**E-mail:** koenraad allemeersch@privacycommission be

Kamer van Vertegenwoordigers
Ter attentie van Mijnheer Siegfried Bracke
Natieplein, 2
1008

| Uw kenmerk | Ons kenmerk | Bijlage(n) | Datum |
|---|---|---|---|
| | SA2/CO-A-2017-001/23 | | 01-03-2017 |

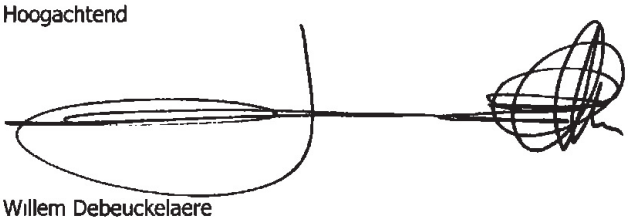
**Betreft:** Wetsvoorstel betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Justitie in het kader van de uitvoering van vrijheidsstraffen en vrijheidsbenemende maatregelen en van het beheer van de inrichtingen waar deze uitvoering plaatsvindt

Mijnheer de Voorzitter

Ik heb de eer u als bijlage kopie te laten geworden van het advies nr. 10/2017 dat de Commissie aangaande bovenvermeld onderwerp op 22 februari 2017 uitbracht.

Zoals voorzien in artikel 29, § 5, 2de lid van de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* wordt terzelfdertijd een kopie van dit advies gezonden aan de Minister van Justitie.

Hoogachtend



Willem Debeuckelaere
Voorzitter

Drukpersstraat 35 | B-1000 Brussel | **T** +32 (0)2 274 48 00 | **E-mail** commission@privacycommission be | **Website** www privacycommission.be