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,

(sé)An Machtens (sé) Willem Debeuckelaere