



Avis n° 147/2019 du 4 septembre 2019

Objet : *Projet d'arrêté royal pris en exécution de l'article 5, § 6, de la loi du 5 mai 2019 portant dispositions diverses en matière d'information de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés (CO-A-2019-156)*

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le 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, ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis du Ministre de la Justice, reçue le 22 juillet 2019 ;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Émet, le 4 septembre 2019, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 22 juillet 2019, le Ministre de la Justice a sollicité l'avis de l'Autorité au sujet d'un Projet d'arrêté royal *pris en exécution de l'article 5, § 6, de la loi du 5 mai 2019 portant dispositions diverses en matière d'information de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés* (ci-après "le Projet").
2. Le Projet vise à préciser les catégories de données visées à l'article 5, §§ 1 à 5 de la loi du 5 mai 2019 *portant dispositions diverses en matière d'information de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés* (ci-après "la loi du 5 mai 2019")¹ et qui sont traitées dans la banque de données "Sidis Suite"². Dans ladite banque de données, des données à caractère personnel de détenus sont traitées par le Service public fédéral Justice et ce service public est également désigné explicitement comme le responsable du traitement à l'article 4 de la loi du 5 mai 2019.
3. Les catégories de données précisées dans le Projet et qui seront dès lors reprises dans la banque de données Sidis Suite portent sur les catégories suivantes de personnes concernées³ : détenus, enfants séjournant auprès de détenus, visiteurs de détenus⁴, autres personnes qui pénètrent dans des établissements pénitentiaires et victimes de détenus.

II. EXAMEN DE LA DEMANDE D'AVIS

4. **Premièrement**, l'Autorité souligne à toutes fins utiles que le Projet relève du champ d'application du RGPD et non - comme on aurait peut-être pu logiquement s'y attendre - du Titre 2 de la LTD⁵. La LTD énumère en effet de manière limitative les services qui relèvent du champ d'application de la Directive Police & Justice⁶ et l'administration pénitentiaire n'y est pas reprise. Dès lors, ses traitements **relèvent du RGPD**⁷.

¹ L'Autorité et son prédécesseur en droit, à savoir la Commission de la protection de la vie privée, se sont déjà prononcées à plusieurs reprises sur les projets de texte qui étaient à la base de la loi du 5 mai 2019 (voir les avis n° 10/2017, 50/2017 & 95/2018).

² L'article 5, § 6 de la loi du 5 mai 2019 prévoit une délégation au Roi pour préciser les catégories de données.

³ Voir l'article 5, §§ 1 à 5 de la loi du 5 mai 2019.

⁴ "Les parents et alliés en ligne directe, le tuteur, le conjoint, le cohabitant légal ou de fait, les frères, les sœurs, les oncles et les tantes sont admis à rendre visite aux détenus (...)" (article 59 de la loi de principes concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, auquel l'article 5, § 3 de la loi du 5 mai 2019 renvoie).

⁵ Voir le point 7 de l'avis n° 95/2018.

⁶ Directive 2016/680/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*.

⁷ Voir l'article 2.2. point d) du RGPD et les articles 25, 26, 7° et 27 de la LTD.

5. **Deuxièmement**, l'Autorité rappelle que l'article 22 de la Constitution interdit au législateur de renoncer à la possibilité de déterminer lui-même quelles ingérences peuvent restreindre le droit au respect de la vie privée⁸. Dans ce contexte, une délégation conférée au Roi *"n'est pas contraire au principe de légalité pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur"*⁹. L'Autorité constate que l'article 5 de la loi du 5 mai 2019 définit effectivement les éléments essentiels des catégories de données qui sont traitées dans Sidis Suite et que la délégation au Roi prévue à l'article 5, § 6 pour la précision de ces catégories (ce qui fait l'objet du Projet – voir les points 1 & 2) **réussit donc le test du principe de légalité**.
6. **Troisièmement**, l'Autorité constate que le Projet décrit quelles données seront reprises dans la banque de données Sidis Suite. Pour autant que l'Autorité puisse en juger¹⁰ et sans préjudice de quelques remarques ponctuelles au point 8, elle n'a pas de remarque particulière quant à la nature des catégories de données qui y sont énumérées. Elle a toutefois une objection de principe quant à la formulation du Projet laissant entendre que les données qui y sont énoncées non sont pas exhaustives. Le choix d'énumérations non limitatives est expliqué comme suit : *"(...) Il est ainsi tenu compte des éventuels oublis et du caractère inévitablement évolutif de chaque banque de données"*¹¹. L'Autorité ne partage pas ce point de vue et souligne que **le but du Projet devrait être précisément de parvenir à une énumération transparente et exhaustive de toutes les données qui sont traitées dans Sidis Suite**. Une énumération non limitative est contraire aux principes de protection des données¹² et empêche la réalisation d'un test de proportionnalité complet au sens de

⁸ Avis n° 63.202/2 du 26 avril 2018 du Conseil d'État émis concernant un avant-projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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, Doc. Parl., Chambre, 54-3185/001, p. 121-122.

Voir dans le même sens les avis suivants du Conseil d'État :

- l'Avis n° 26.198/2 rendu le 2 février 1998 sur un avant-projet de loi qui a conduit à la loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données", Doc. Parl. Chambre, 1997-98, n° 49-1566/1, 108 ;
- l'Avis n° 33.487/1/3 des 18 et 20 juin 2002 relatif à un avant-projet de loi qui a conduit à la loi du 22 août 2002 portant des mesures en matière de soins de santé", Doc. Parl. Chambre 2002-03, n° 2125/2, 539 ;
- l'Avis n° 37.765/1/2/3/4 rendu le 4 novembre 2004 sur un avant-projet de loi-programme qui a donné lieu à la loi-programme du 27 décembre 2004, Doc. Parl. Chambre 2004-05, n° 1437/2.

⁹ Voir également Cour constitutionnelle, Arrêt n° 29/2010 du 18 mars 2010, point B.16.1 ; Arrêt n° 39/2013 du 14 mars 2013, point B.8.1 ; Arrêt n° 44/2015 du 23 avril 2015, point B.36.2 ; Arrêt n° 107/2015 du 16 juillet 2015, point B.7 ; Arrêt n° 108/2017 du 5 octobre 2017, point B.6.4 ; Arrêt n° 29/2010 du 15 mars 2018, point B.13.1 ; Arrêt n° 86/2018 du 5 juillet 2018, point B.7.2. ; Avis du Conseil d'État n° 63.202/2 du 26 avril 2018, point 2.2.

¹⁰ Le responsable du traitement – à savoir le SPF Justice – est en effet le mieux placé pour déterminer quelles données sont nécessaires pour atteindre les finalités envisagées.

¹¹ P. 2 du Rapport au Roi du Projet.

¹² Voir l'article 6.3 du RGPD, lu conjointement avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales.

l'article 5.1.c) du RGPD. S'il est un fait que la banque de données Sidis Suite évoluera inévitablement dans le temps, il convient alors de prévoir une évolution similaire du contenu de l'arrêté d'exécution dans lequel les catégories de données sont précisées.

7. Parallèlement, l'Autorité fait également remarquer que le Projet n'exécute que l'article 5, § 6 de la loi du 5 mai 2019, alors que cette loi prévoit aussi d'autres délégations au pouvoir exécutif dont la concrétisation aura un impact significatif sur la proportionnalité des traitements envisagés¹³. Elle recommande dès lors de rédiger le Projet parallèlement à ces autres arrêtés d'exécution, afin de pouvoir réaliser un test de proportionnalité complet.
8. **Quatrièmement**, l'Autorité a quelques remarques ponctuelles quant aux notions suivantes que l'on retrouve dans le Projet :
 - les termes "numéro d'identification de la sécurité sociale" et "numéro bis" sont mentionnés dans plusieurs articles et l'Autorité recommande de les harmoniser avec la formulation utilisée à l'article 8 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* ;
 - on ne comprend pas clairement ce que l'on vise par la notion de "plan de détention individuel"¹⁴. Si ce terme n'est pas défini dans une autre réglementation, l'Autorité demande d'en prévoir une définition dans le Projet.
9. **Cinquièmement**, l'Autorité attire l'attention sur l'article 32 du RGPD, qui impose au responsable du traitement de **prendre les mesures techniques et organisationnelles requises** pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de sécurité approprié, compte tenu, d'une part, de l'état des connaissances en la matière et des coûts qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
10. L'article 32 du RGPD se réfère à cet égard à plusieurs exemples de mesures afin d'assurer, au besoin, un niveau de sécurité adapté au risque :
 - la pseudonymisation et le chiffrement des données à caractère personnel ;

¹³ L'article 7, § 2 de la loi du 5 mai 2019 prévoit par exemple encore une délégation au Roi pour déterminer les finalités pour lesquelles les organisations énoncées à l'article 7, § 1 de cette loi peuvent exercer leur droit de lecture dans Sidis Suite. Et l'article 9 de la loi du 5 mai 2019 dispose que le Roi doit énoncer les modalités relatives à la période durant laquelle les données doivent être disponibles et consultables dans Sidis Suite. C'est surtout le contenu du premier arrêté d'exécution qui est important pour pouvoir réaliser un test de proportionnalité relatif aux données qui seront traitées dans Sidis Suite en vertu du Projet.

¹⁴ Article 2, § 3, 3° du Projet.

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes de traitement ;
 - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
11. Pour l'exécution concrète de ces mesures, l'Autorité renvoie à la recommandation de la Commission de la protection de la vie privée¹⁵ visant à prévenir les fuites de données et au document "Mesures de référence¹⁶ en matière de sécurité applicables à tout traitement de données à caractère personnel". L'Autorité souligne également l'importance d'une bonne gestion des utilisateurs et des accès¹⁷.
12. Les catégories particulières de données à caractère personnel au sens des articles 9 et 10 du RGPD requièrent des mesures de sécurité plus strictes. Les articles 9 et 10, § 2 de la LTD indiquent quelles mesures de sécurité supplémentaires devront au moins être prévues :
- désigner les catégories de personnes, ayant accès aux données à caractère personnel, avec une description précise de leur fonction par rapport au traitement des données visées ;
 - tenir la liste des catégories des personnes ainsi désignées à la disposition de l'Autorité ;
 - veiller à ce que ces personnes désignées soient tenues par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

¹⁵ Voir également la recommandation d'initiative de la Commission de la protection de la vie privée n° 01/2013 du 21 janvier 2013 *relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf).

¹⁶ Mesures de référence de la Commission de la protection de la vie privée en matière de sécurité applicables à tout traitement de données à caractère personnel, Version 1.0,

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_scurite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf).

¹⁷ Voir également la recommandation de la Commission de la protection de la vie privée n° 01/2008 du 24 septembre 2008 *relative à la gestion des accès et des utilisateurs dans le secteur public*

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2008_0.pdf).

Plusieurs instances peuvent proposer à cet effet des solutions technologiques adaptées (comme par exemple la Banque carrefour de la Sécurité Sociale).

PAR CES MOTIFS,

l'Autorité estime que les adaptations suivantes du Projet s'imposent :

- fixer de manière limitative les catégories des données à caractère personnel traitées (points 6-7) ;
- adapter/définir les notions de "numéro d'identification de la sécurité sociale", "numéro bis" et "plan de détention individuel", comme exposé au point 8.

l'Autorité attire l'attention du demandeur sur l'importance des éléments suivants :

- le respect de l'article 32 du RGPD et l'obligation du responsable du traitement de prendre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel (points XXX).

(sé) Alexandra Jaspar

Directrice du Centre de Connaissances