Avis n° 116/2019 du 5 juin 2019

Objet : Avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel réalisés par le Service public fédéral Justice dans le cadre de ses missions (CO-A-2019-117)

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 de Monsieur Koen Geens, Ministre de la Justice, reçue le 4 avril 2019 ;

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

Émet, le 5 juin 2019, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le Ministre de la Justice, Koen Geens, (ci-après : le demandeur) sollicite l'avis de l'Autorité sur un avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel réalisés par le Service public fédéral Justice dans le cadre de ses missions (ci-après : l'avant-projet).

Contexte

2. L'avant-projet crée un cadre général pour le traitement de données à caractère personnel par le Service public fédéral Justice (ci-après : le SPF Justice), par analogie avec la loi du 3 août 2012 *portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions* (ci-après : la loi du 3 août 2012) qui crée un cadre similaire pour le SPF Finances[1]. L'article 3 de l'avant-projet précise que ce cadre général ne s'applique que dans la mesure où un traitement du SPF Justice ne résulte pas d'une législation particulière. L'avant-projet exclut l'ordre judiciaire de son champ d'application.

3. En substance, les dispositions de l'avant-projet régissent les cinq questions suivantes :

- les conditions pour le traitement de données à caractère personnel au sein du SPF Justice ;
- les conditions pour l'échange de données à caractère personnel avec d'autres SPF ;
- la création d'un Service de la Sécurité de l'Information et de la Protection des données au sein du SPF Justice ;
- la création d'un datawarehouse au sein du SPF Justice ;
- une limitation extrême des droits de la personne concernée.

4. Vu le lien étroit entre l'avant-projet et la loi du 3 août 2012, l'Autorité tient particulièrement compte, dans le présent avis, des dispositions de cette loi ainsi que des avis que la Commission de la protection de la vie privée (ci-après : la Commission), a émis en amont de sa réalisation :

- l'avis n° 01/2007 du 17 janvier 2007[2] ;
- l'avis n° 16/2007 du 11 avril 2007[3] ;

---

[1] Loi du 3 août 2012 *portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions*, *M.B.* du 24 août 2012.

[2] Avis n° 01/2007 de la Commission du 17 janvier 2007, disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_01_2007.pdf.

[3] Avis n° 16/2007 de la Commission du 11 avril 2007, disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_16_2007_0.pdf.

- l'avis n° 11/2012 du 11 avril 2012[4].

II. EXAMEN DE LA DEMANDE D'AVIS

1. Fondement juridique

5. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD. En outre, le traitement de catégories particulières de données à caractère personnel est interdit en vertu de l'article 9.1 du RGPD, sauf si le responsable du traitement peut invoquer un des motifs de légitimation de l'article 9.2 du RGPD. Le traitement de données pénales est uniquement possible selon les conditions définies à l'article 10 du RGPD.

6. Dans la mesure où le traitement de données à caractère personnel par le SPF Justice ne concerne pas des catégories particulières de données à caractère personnel ou des données pénales, l'avant-projet peut reposer sur l'article 6.1.e) du RGPD : le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

7. L'Autorité souligne dès lors l'importance de l'article 6.3 du RGPD qui - lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution - prescrit que la réglementation qui encadre des traitements au sens de l'article 6.1.e) du RGPD devrait au moins mentionner les éléments essentiels suivants de ces traitements :
    - la finalité du traitement ;
    - les types ou catégories de données à caractère personnel qui feront l'objet du traitement. Ces données doivent en outre être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données") ;
    - les personnes concernées ;
    - les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
    - les durées de conservation ;
    - la désignation du ou des responsables du traitement.

8. L'Autorité constate que l'avant-projet ne désigne en aucune façon les catégories de données à caractère personnel qui feront l'objet du traitement, ce qui empêche d'évaluer si l'avant-projet doit définir une base juridique pour le traitement de catégories particulières de

[4] Avis n° 11/2012 de la Commission du 11 avril 2012, disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_11_2012_0.pdf.

données à caractère personnel ou de données pénales. Cette lacune a pour conséquence que - dans la mesure où une législation particulière ne prévoit pas une telle base juridique - le traitement de catégories particulières de données à caractère personnel et de données pénales par le SPF Justice dans le cadre du présent avant-projet est contraire au RGPD.

2. Finalité

9. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel est exclusivement autorisé pour des finalités déterminées, explicites et légitimes.

10. L'article 4 de l'avant-projet dispose que le SPF Justice collecte et traite des données à caractère personnel "*afin d'exécuter ses missions légales*". L'Exposé des motifs explique qu'une énumération exhaustive de ces missions légales n'est pas souhaitable car cela donnerait lieu à une liste incomplète et nécessiterait en outre une mise à jour constante de la loi. Bien qu'une énumération exhaustive de toutes les missions légales ne soit pas nécessaire, l'avant-projet doit toujours préciser suffisamment les finalités du traitement.

11. Cette précision est nécessaire notamment pour pouvoir évaluer dans quelle mesure l'avant-projet doit être confronté au RGPD ou à la Directive[5]. En effet, les dispositions introductives de l'Exposé des motifs renvoient certes de manière circonstanciée à la Directive et au RGPD, sans toutefois préciser dans quelle mesure l'avant-projet relève du champ d'application soit de la Directive, soit du RGPD. En l'absence de détermination des finalités, il est toutefois impossible de définir ce cadre d'évaluation. L'Autorité attire en outre l'attention du demandeur sur le fait que le SPF Justice n'est pas une autorité compétente telle que définie à l'article 26, 7° de la LTD[6]. Dès lors, en vertu de l'article 27 de la LTD, le titre 2 de cette même loi pourrait même ne pas s'appliquer du tout. Néanmoins, l'Exposé des motifs et l'avant-projet renvoient parfois à des dispositions reprises au titre 2 de la LTD, ce qui soulève davantage la question de la portée précise de l'avant-projet.

12. Étant donné l'absence de définition d'une finalité claire à l'article 4 de l'avant-projet, la création prévue d'un datawarehouse doit être qualifiée de manifestement contraire au RGPD. Une finalité déterminée constitue en effet un élément essentiel qui doit être défini dans la base juridique (article 6.3 du RGPD). C'est effectivement en fonction de la finalité déterminée

[5] Directive (UE) 2016/680 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* (ci-après "la Directive").

[6] L'article 26, 7°, b) mentionne "*les autorités judiciaires, entendues comme les cours et tribunaux du droit commun et le ministère public*" mais l'article 3 de l'avant-projet exclut l'ordre judiciaire de son champ d'application.

que l'on peut notamment vérifier la proportionnalité des données pouvant entrer en ligne de compte pour être reprises dans ce datawarehouse, que l'on peut contrôler la compatibilité d'éventuels traitements ultérieurs et que l'on doit évaluer la pertinence de l'accès aux données par certaines personnes. L'article 7, § 1er de l'avant-projet stipule simplement que l'agrégation de données à caractère personnel se fait dans le datawarehouse "*en vue de réaliser, dans le cadre de ses missions légales, des analyses sur des données relationnelles*". Dans son avis n° 34/2018 du 11 avril 2018, la Commission a estimé que la finalité de "*datamatching et de dataming en vue d'une lutte efficace contre la fraude sociale*" était formulée de manière trop large pour fournir au justiciable des précisions quant aux circonstances exactes de la collecte de ses données à caractère personnel dans un datawarehouse[7]. Le présent avant-projet ne prévoit aucune finalité, rendant tout à fait impossible l'évaluation de la proportionnalité de cette mesure. À cet égard, l'Autorité attire en outre l'attention sur l'arrêt n° 29/2018 dans lequel la Cour constitutionnelle affirmait que l'exigence d'une base légale prévisible précise (et donc une finalité claire) "*[s'applique] d'autant plus lorsque les données à caractère personnel sont ensuite traitées par les services publics à d'autres fins que celles pour lesquelles elles ont initialement été obtenues*"[8].

13. L'Autorité constate que la finalité est moins bien définie - tout simplement pas du tout - que les formulations que la Commission a déjà rejetées par le passé, alors que l'exigence constitutionnelle de prévisibilité doit précisément être appliquée de manière plus stricte en vertu de la jurisprudence de la Cour constitutionnelle. L'avant-projet doit donc établir pour quelles finalités spécifiques le datawarehouse traitera des données à caractère personnel. Ainsi, l'article 5, § 1er de la loi du 3 août 2012 et l'article 5*bis* de la loi du 15 janvier 1990[9] précisent que les datawarehouses du SPF Finances et des institutions de sécurité sociale servent respectivement "*en vue de réaliser les finalités de contrôles ciblés sur la base d'indicateurs de risque*", ou "*en vue de la prévention, de la constatation, de la poursuite et de la répression des infractions sur la réglementation sociale qui relèvent de leurs compétences respectives et en vue de la perception et du recouvrement des montants*". Ni l'avant-projet lui-même, ni l'Exposé des motifs ne donnent ici la moindre précision, l'article 7 de l'avant-projet étant ainsi en contradiction flagrante avec l'article 5.1.b) du RGPD.

---

[7] Avis n° 34/2018 de la Commission du 11 avril 2018, disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_34_2018.pdf.

Voir également l'avis n° 99/2019 de l'Autorité du 3 avril 2019, dans lequel l'Autorité estimait que la finalité "*la réalisation de recherches pouvant être utiles à la connaissance, à la conception et à la gestion de la protection sociale*" était définie de manière trop vague, disponible à l'adresse suivante :

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_99_2019.pdf.

[8] Cour constitutionnelle du 15 mars 2018, arrêt n° 29/2018, B.18.

[9] Loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, , *M.B.* du 22 février 1990.

14. L'article 4, § 1er de l'avant-projet dispose ensuite que le SPF Justice "*peut traiter ultérieurement pour l'exécution d'une autre mission légale toute donnée à caractère personnel collectée légitimement dans le cadre de l'exécution de l'une de ses autres missions légales*", certes en tenant compte du contrôle de compatibilité figurant aux articles 6.4 du RGPD et 29 de la LTD. Dans son avis n° 16/2007, la Commission a estimé que le contrôle de la compatibilité était une garantie indispensable qui devait accompagner la libre circulation de données à caractère personnel au sein du SPF Finances[10]. L'Autorité souligne que le SPF Justice, en tant que responsable du traitement, doit toujours documenter l'analyse sous-jacente de ce contrôle de compatibilité et, le cas échéant, la soumettre à l'Autorité. Bien que dans son avis n° 11/2012, la Commission ait approuvé une disposition formulée de manière similaire[11], la lecture conjointe des articles 4 et 7 du présent avant-projet va à l'encontre du principe de limitation des finalités. En effet, la lecture de l'avant-projet implique que le SPF Justice pourrait traiter ultérieurement dans son datawarehouse toutes les données à caractère personnel qu'il reçoit dans le cadre de ses missions légales pour des missions légales que l'avant-projet ne précise pas davantage. De cette façon, ni l'Autorité, ni le justiciable ne peuvent évaluer si ces traitements ultérieurs sont nécessaires et proportionnels.

15. L'Autorité constate que la définition des finalités poursuivies fait défaut ; il manque donc un des éléments essentiels que le législateur est tenu de définir dans sa base juridique (voir le point 7). En ne définissant aucune finalité, l'avant-projet risque de conduire à une confusion de finalités et à un "function creep" (détournement d'usage) pour lesquels la Commission a formulé des avertissements dans son Rapport Big Data[12].

3. Proportionnalité

16. L'article 5.1.c) du RGPD dispose que les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données").

17. On peut déduire de l'avant-projet qu'il couvre un éventail de divers traitements de données à caractère personnel. Derrière la notion de "missions légales", se cachent en effet toute une série de finalités. En raison du fait que l'avant-projet ne définit ni les catégories de données à caractère personnel, ni les finalités du traitement de celles-ci, il est impossible d'évaluer la nécessité et la proportionnalité. L'Autorité rappelle que les catégories de données à caractère

[10] Avis n° 16/2007, point 8.

[11] Avis n° 11/2012, point 6.

[12] Commission, Rapport Big Data, page 42, disponible à l'adresse suivante : https://www.privacycommission.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf.

personnel constituent des éléments essentiels qui, selon l'article 22 de la Constitution, doivent être définis dans la loi formelle[13].

18. L'article 7, § 3 de l'avant-projet dispose que pour l'ajout de toute catégorie de données à caractère personnel, l'avis du Service de la Sécurité de l'Information et de la Protection des données au sein du SPF Justice est toujours nécessaire. Le demandeur doit compléter l'avant-projet en précisant explicitement que lorsque les données à caractère personnel proviennent d'un tiers, la délibération du comité de sécurité de l'information compétent est également requise. Dans son avis n° 11/2012, la Commission avançait déjà cette exigence[14] et l'article 5, § 2 de la loi du 3 août 2012 stipule également que l'ajout de toute catégorie de données à caractère personnel par un tiers ne peut se faire qu'après une délibération du comité de sécurité de l'information. Ceci doit permettre d'évaluer la proportionnalité en détail.

19. L'Autorité répète que l'avant-projet ne fait pas la moindre allusion au traitement de catégories particulières de données à caractère personnel, ni aux données pénales[15]. Vu la définition de la mission du SPF Justice à l'article 2, § 1er de l'arrêté royal du 23 mai 2001[16], le traitement de ces données à caractère personnel sensibles est pourtant indispensable pour réaliser les missions du SPF Justice. Le traitement de ces données ressort aussi implicitement de l'article 6, § 1er, 1° de l'avant-projet sans qu'il ne soit toutefois précisé quelque part de quelles données à caractère personnel il s'agit précisément, ni sous quelles conditions le SPF Justice traite ces données à caractère personnel sensibles. Un cadre général qui régira tous les traitements de données à caractère personnel par le SPF Justice doit également prévoir les garanties complémentaires nécessaires pour le traitement de ces données à caractère personnel en particulier[17].

4. Délai de conservation

20. Selon l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

---

[13] Avis n° 34/2018, point 31.

[14] Avis n° 11/2012, point 16.

[15] Implicitement, on peut toutefois déduire de l'article 6 de l'avant-projet que le demandeur vise bel et bien le traitement de ces données à caractère personnel, ce qui fait de l'absence de définition plus détaillée de ces données et des garanties y afférentes un obstacle d'autant plus sérieux.

[16] Arrêté royal du 23 mai 2001 *portant création du Service public fédéral Justice*, *M.B.* du 29 mai 2001.

[17] L'Autorité pense par exemple aux données de santé de détenus, dont le traitement n'est pas rigoureusement régi par la loi de principes du 12 janvier 2005 *concernant l'administration pénitentiaire ainsi que le statut juridique des détenus*, *M.B.* du 1er février 2005.

21. L'article 4, § 2, premier alinéa de l'avant-projet répète simplement l'article 5.1.e) du RGPD et est ainsi contraire à l'interdiction de retranscription du RGPD. Le demandeur doit supprimer cet alinéa. Outre un délai de conservation maximal de 5 ans, l'avant-projet définit également un délai de conservation maximal particulier de 10 ans pour les dossiers de contentieux. L'avant-projet doit établir quand ces délais de conservation de 5 et 10 ans commencent précisément à courir. Par ailleurs, l'Exposé des motifs doit indiquer pour quelles raisons le délai de conservation pour les dossiers de contentieux est plus long que le délai de conservation général de 5 ans.

22. L'article 4, § 2, quatrième alinéa de l'avant-projet affirme ensuite que ces délais peuvent systématiquement être prolongés de 5 ans, sans toutefois pouvoir dépasser un délai de conservation maximum de 30 ans. Afin de déterminer si le SPF Justice conservera les données à caractère personnel pour un délai supplémentaire de 5 ans, il réalise une analyse "*sur base de différents critères de nécessité et de proportionnalité*". Le Service de la Sécurité de l'Information et de la Protection des données au sein du SPF Justice émet un avis sur ces critères. Bien que l'Autorité ne soit pas réticente à cette forme de conservation par paliers, elle estime toutefois nécessaire de déterminer les critères dans la loi et de mieux justifier le délai de conservation maximum dans l'Exposé des motifs.

23. L'article 7, § 2 de l'avant-projet dispose que, sans préjudice de la conservation nécessaire pour les finalités mentionnées à l'article 89 du RGPD, les données à caractère personnel qui résultent des traitements dans le datawarehouse "*ne sont pas conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées*". Le rapport entre les délais de conservation aux articles 4 et 7 de l'avant-projet n'est pas clair - l'article 7, § 2 constitue-t-il une *lex specialis* par rapport à l'article 4 ou non ? En outre, les finalités pour le traitement par le datawarehouse n'ont pas été déterminées, ce qui implique que le délai de conservation reste également indéterminé. De nouveau, l'avant-projet omet de définir un des éléments essentiels qui sont nécessaires pour déterminer le fondement juridique pour le datawarehouse. À cet égard, l'Autorité attire l'attention sur le fait que tant l'article 5, § 1er de la loi du 3 août 2012 que l'article 5*bis* de la loi du 15 janvier 1990 prévoient un délai maximal de conservation d'un an après la prescription de toutes les actions qui relèvent de la compétence du responsable du traitement pour les données à caractère personnel résultant d'un traitement du datawarehouse.

5. Échange de données interne et externe

24. L'article 5 de l'avant-projet dispose qu'un règlement décrit le processus de demande et d'accès aux données à caractère personnel au sein du SPF Justice (échange de données interne).

L'article n'indique pas qui adopte ce règlement. De plus, l'avant-projet met la barre plus bas que pour le SPF Finances pour qui ce règlement doit être approuvé par le Roi. L'Autorité recommande de mieux aligner l'article 5 de l'avant-projet sur le règlement repris à l'article 4 de la loi du 3 août 2012 et, par analogie, de soumettre également ce règlement à l'approbation du Roi.

25. L'article 6 de l'avant-projet dispose que le SPF Justice ne transmet des données à caractère personnel à "*un autre service public ou à une personne morale de droit public ou privé, ou un tiers*" ou ne reçoit de telles données de ces organismes qu'après avis du Service de la Sécurité de l'Information et de la Protection des données au sein du SPF Justice. Les § 1er et 2 de l'article 6 de l'avant-projet spécifient ensuite qu'un protocole au sens de l'article 20 de la LTD doit également encadrer cette transmission dans seulement trois cas :

- lors du traitement de catégories particulières de données à caractère personnel ou de données pénales ;
- lorsque les données traitées sont systématiques ou volumineuses ;
- lorsqu'il découle d'une analyse d'impact relative à la protection des données que le transfert comporte un risque élevé pour les droits des personnes concernées.

26. À cet égard, l'article 6 de l'avant-projet est très problématique car cette disposition déroge au champ d'application de l'article 20 de la LTD, sans toutefois justifier pourquoi le SPF Justice a besoin d'un régime spécifique moins strict pour la transmission de données à caractère personnel. L'absence d'un protocole d'accord et de publication de celui-ci sur le site Internet des responsables du traitement concernés prive en outre le justiciable d'une importante garantie en matière de transparence. Dans ce contexte, l'Autorité attire l'attention sur l'arrêt *Smaranda Bara* de la Cour de justice qui a rappelé que la directive 95/46 s'opposait "*à des mesures nationales [...] qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission et de ce traitement*"[18]. En l'occurrence, il s'agissait d'une transmission en vertu d'un protocole non publié entre le fisc roumain et les services de la sécurité sociale. Cependant, l'article 6 de l'avant-projet crée même des situations dans lesquelles aucun protocole d'accord ne serait requis. Par conséquent, le justiciable ne pourra raisonnablement pas prévoir, ni sur la base d'une lecture de l'article 6 de l'avant-projet, ni sur la base d'un protocole publié, que certaines transmissions auront lieu au départ et vers le SPF Justice.

[18] Cour de justice, 1er octobre 2015 , *Smaranda Bara e.a.* (C-201/14), § 46.

27. En d'autres termes, l'obligation de conclure un protocole d'accord constitue une exigence minimale de transparence et ne peut pas être réduite, de façon conceptuelle, à une mesure de sécurité qui ne serait nécessaire qu'en cas de risque accru du traitement. Il s'agit d'une garantie juridique pour chaque justiciable qui doit permettre un contrôle de l'ingérence des pouvoirs publics dans sa vie privée. Ceci a également été souligné par le Conseil d'État dans son avis sur la LTD : "*Étant donné que ces protocoles organisent une ingérence dans la vie privée, ils doivent être accessibles pour les personnes concernées en vertu de l'article 22 de la Constitution de manière à assurer la prévisibilité des transferts et des traitements.*"[19].

28. L'article 6 de l'avant-projet repose dès lors sur une erreur conceptuelle concernant la *ratio legis* qui sous-tend l'article 20 de la LTD et doit donc être supprimé dans la mesure où il réduit l'obligation de conclure un protocole d'accord à seulement trois cas types.

29. Enfin, l'Autorité attire l'attention sur le flou terminologique à l'article 6 de l'avant-projet. Cet article parle de transmissions au départ de et vers "*un autre service public ou une personne morale de droit public ou privé, ou un tiers*" alors que l'article 20 de la LTD fait mention de transmissions entre "*l'autorité publique fédérale*" et "*toute autre autorité publique ou organisation privée*". L'Autorité ne sait pas non plus clairement à quels acteurs la notion de "*tiers*" figurant à l'article 6 de l'avant-projet se rapporte précisément.

6. Service de la Sécurité de l'Information et de la Protection des données

30. L'article 8 de l'avant-projet crée au sein du SPF Justice le Service de la Sécurité de l'Information et de la Protection des données. L'avant-projet précise que ce service assume le rôle de délégué à la protection des données. À l'instar des lignes directrices du Groupe de protection des données Article 29, l'Autorité fait remarquer que le choix de ce service qui assume dans son intégralité le rôle de délégué à la protection des données implique que chaque membre doit remplir l'ensemble des exigences applicables établies à la section 4 du RGPD[20]. Cela implique également que le Service de la Sécurité de l'Information et de la Protection des données ne peut assumer aucune tâche qui serait en conflit avec le rôle de délégué à la protection des données. Sur ce point, l'Autorité fait remarquer qu'en vertu de l'article 30 du RGPD, la gestion du registre des activités de traitement est une tâche qui repose sur le responsable du traitement lui-même et pas sur le délégué à la protection des données (voir également à cet égard le point 40). Pour le reste, l'article 8 de l'avant-projet répète aussi plusieurs tâches qui découlent directement du RGPD et qui doivent dès lors être supprimées.

---

[19] Conseil d'État du 19 avril 2018, avis n° 63.192/2, page 23.

[20] Groupe de protection des données Article 29, 5 avril 2017, "Lignes directrices concernant les délégués à la protection des données (DPD)", WP 243 rev.01, page 14.

7. Limitation des droits de la personne concernée

31. L'article 12 de l'avant-projet établit qu'outre les éléments mentionnés à l'article 13 du RGPD, plusieurs éléments d'information complémentaires sont mentionnés sur le site Internet du SPF Justice. L'Exposé des motifs explique que cette disposition sert "*afin de garantir le droit à l'information de la personne concernée tel que prévu aux articles 12, 13 et 14 du RGPD*". Le texte de l'article 12 de l'avant-projet ne renvoie ni à l'article 12, ni à l'article 14 du RGPD. Le demandeur doit rectifier cette lacune.

32. L'article 13 de l'avant-projet prévoit des limitations aux droits de la personne concernée, à savoir : le droit d'obtenir dans un délai d'un mois une réponse du responsable du traitement, le droit d'accès, le droit de rectification, le droit à la limitation du traitement, l'obligation de notification et le droit d'opposition. En outre, les paragraphes 2 et 3 de l'article 13 de l'avant-projet limitent respectivement le droit à l'information dans le cadre de l'obtention indirecte des données à caractère personnel et le droit à l'oubli. Enfin, le § 4 de l'article 13 de l'avant-projet autorise la prise de décision automatisée.

33. En vertu de l'article 14, § 1er de l'avant-projet, la limitation de ces droits ne s'applique pas dans la mesure où cette application :
    - nuirait aux besoins de la prévention et [de] la détection d'infractions pénales, ainsi que [des] enquêtes et [des] poursuites en la matière ou [de] l'exécution de sanctions pénales ;
    - implique une prise de connaissance par la personne concernée qui porterait gravement atteinte à la sécurité d'une autre personne ;
    - pourrait nuire à la confidentialité d'un dossier relatif à des affaires de contentieux.

34. Toute mesure législative prévoyant des limitations aux droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, comme :

    - les finalités (des catégories) du traitement ;
    - les catégories de données à caractère personnel ;
    - l'étendue des limitations ;
    - les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
    - la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement) ;
    - les durées de conservation ;
    - les risques pour les droits et libertés des personnes concernées et
    - le droit de la personnes concernée d'être informée de la limitation.

35. L'actuel avant-projet et l'Exposé des motifs omettent d'indiquer concrètement la nécessité et les finalités de l'application de ces limitations. Certes, l'Exposé des motifs mentionne la nécessité de suspendre le droit d'accès pour les dossiers d'extradition, les mandats d'arrêt et les demandes de rectification dans le Moniteur belge mais n'explique pas pourquoi ces trois situations justifient par exemple l'exclusion de tous les autres droits mentionnés à l'article 13 de l'avant-projet. La portée de l'exclusion des droits de la personne concernée est dès lors disproportionnée.

36. L'avant-projet ne détermine pas les catégories de données à caractère personnel auxquelles se rapportent les exceptions, ni le champ d'application précis de celles-ci. La formulation actuelle de ces limitations ne constitue donc pas une mesure légitime qui soit raisonnablement prévisible pour la personne concernée. Le demandeur doit indiquer et expliquer de manière cohérente dans l'Exposé des motifs de quelle manière l'avant-projet couvre les éléments repris à l'article 23.2 du RGPD.

37. L'avant-projet contient également des contradictions étant donné qu'il exclut d'une part l'application de l'article 12.3 du RGPD (l'obligation de communiquer des informations dans un délai d'un mois) pour ensuite réinstaurer une obligation quasi identique via l'article 14, § 6. Comment le législateur peut-il alors justifier la nécessité d'exclure l'article 12.3 du RGPD mentionnée en premier lieu ?

38. En outre, l'avant-projet ne développe pas non plus de justification suffisante pour suspendre l'interdiction de prise de décisions automatisée de l'article 22 du RGPD. Les conditions énumérées à l'article 14, § 1er de l'avant-projet ne semblent pas pouvoir justifier qu'une personne puisse être soumise à une forme de prise de décision automatisée. Il ressort de l'Exposé des motifs que cette exception doit être examinée en relation avec le fonctionnement du datawarehouse, sans toutefois expliquer pourquoi une exception à cette interdiction est nécessaire. En effet, le simple fonctionnement d'un datawarehouse n'implique pas nécessairement une prise de décision automatisée sans intervention humaine telle que visée à l'article 22 du RGPD. Qui plus est, l'Exposé des motifs indique précisément qu'il y aura toujours une intervention humaine avant qu'une décision ne soit prise. L'exclusion de l'interdiction à l'article 22 du RGPD semble dès lors reposer sur une lecture erronée du RGPD lui-même.

39. L'avant-projet et l'Exposé des motifs partent du principe que certaines exceptions aux droits de la personne concernée s'appliquent directement, sans qu'il ne faille remplir les conditions de l'article 23 du RGPD. À cet égard, l'Autorité rappelle l'avis n° 41/2018 de la Commission dans lequel cette dernière affirme que ce raisonnement ne tient pas debout pour la mise en

œuvre des articles 14.5.c) 17.3.b) du RGPD par exemple. Cela aurait en effet pour conséquence indésirable que les garanties découlant de l'article 23 du RGPD seraient annulées pour une sélection déterminée de droits[21]. Le législateur doit dès lors lire chacune des sous-exceptions découlant directement des articles de loi spécifiques des articles 12 à 22 inclus du RGPD conjointement avec les exigences découlant de l'article 23 du RGPD.

40. Le demandeur doit également vérifier dans quelle mesure les exceptions qu'il souhaite mettre en place sont déjà couvertes par l'article 14 de la LTD qui prévoit des exceptions aux droits de la personne concernée en matière de données à caractère personnel émanant des autorités judiciaires.

41. L'article 14, § 6 de l'avant-projet dispose que le Service de la Sécurité de l'Information et de la Protection des données se charge d'informer la personne concernée en temps opportun. En vertu de l'article 12 du RGPD, cette obligation revient toutefois au responsable du traitement lui-même et pas au délégué à la protection des données. Le rôle que l'avant-projet réserve au Service de la Sécurité de l'Information et de la Protection des données entre en conflit avec le rôle de délégué à la protection des données et déresponsabilise en même temps le responsable du traitement.

8. Autres remarques

42. Le demandeur doit examiner en profondeur la concordance des textes, étant donné que l'avant-projet contient plusieurs erreurs de traduction, comme par exemple :
    - L'article 3 de l'avant-projet qui traduit "*tout traitement*" par "*enige verwerking*";
    - L'article 6 de l'avant-projet qui traduit "*personne morale de droit public ou privé*" par "*rechtspersoon van publiek of privérecht*".

43. L'article 16 de l'avant-projet établit que l'Autorité de protection des données intervient en tant qu'autorité de contrôle pour le SPF Justice. Vu l'article 4, § 2, deuxième phrase de la LCA, cette disposition ne présente aucune valeur ajoutée et doit dès lors être supprimée.

[21] Avis n° 41/2018 de la Commission du 23 mai 2018, disponible à l'adresse suivante : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_41_2018_0.pdf.

PAR CES MOTIFS,

l'Autorité juge que les adaptations suivantes s'imposent :

- définir un fondement légal pour le traitement de catégories particulières de données à caractère personnel et de données pénales (point 8) ;
- définir les finalités du traitement (point 10) ;
- définir les finalités spécifiques pour le datawarehouse (points 12-15) ;
- définir les catégories de données à caractère personnel qui font l'objet du traitement, avec une attention spéciale pour les catégories particulières de données à caractère personnel et les données pénales (point 17) ;
- subordonner l'ajout d'une catégorie de données par un tiers à une délibération du comité de sécurité de l'information (point 18) ;
- supprimer le premier alinéa du § 2 de l'article 4 de l'avant-projet (point 21) ;
- à l'article 4, § 2, quatrième alinéa, définir et justifier les critères de nécessité et de proportionnalité (point 22) ;
- définir un délai de conservation pour les données à caractère personnel qui font l'objet du traitement résultant du datawarehouse (point 23) ;
- établir que le règlement pour la demande et l'accès aux données à caractère personnel est approuvé par le Roi (point 24) ;
- supprimer l'article 6 de l'avant-projet (point 28) ;
- adapter les missions du Service de la Sécurité de l'Information et de la Protection des données afin qu'il n'y ait plus de conflit avec le rôle de ce service en tant que délégué à la protection des données (point 30) ;
- faire en sorte que les limitations aux droits des personnes concernées soient conformes à l'article 23.2 du RGPD (points 31-41) ;
- supprimer l'article 16 de l'avant-projet (point 43).

(sé) An Machtens
Administratrice f.f.

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances