Avis n° 98/2019 du 3 avril 2019

Objet: Avant-projet de décret relatif aux traitements de données à caractère personnel réalisés par l'entreprise publique des technologies numériques de l'information et de la communication de la communauté française (ETNIC) ou confiés par ses bénéficiaires (CO-A-2019-068).

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

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

Vu la demande d'avis du Ministre de la Fonction publique, du budget et de la simplification administrative du Gouvernement de la Fédération Wallonie-Bruxelles reçue le 13 février 2019;

Vu le rapport de Monsieur Debeuckelaere Willem;

Émet, le 3 avril 2019, l'avis suivant :

I. OBJET DE LA DEMANDE

1. L' Entreprise publique des Technologies Numériques de l'Information et de la Communication de la Communauté française (ci-après l'« ETNIC ») est l'organisme d'intérêt public doté de la personnalité juridique visé par le décret du 25 octobre 2018 *relatif à l'Entreprise publique des Technologies Numériques de l'Information et de la Communication de la Communauté française* (ci-après « décret ETNIC »). Les bénéficiaires des missions de l'ETNIC (ci-après les « bénéficiaires ») sont désignés à l'article 1er, 2°, du décret ETNIC .

2. L'avant-projet de décret *relatif aux traitements de données à caractère personnel réalisés par l'ETNIC ou confiés par ses bénéficiaires* (ci-après « avant-projet de décret ») a pour objectif d'encadrer les rapports entre l'ETNIC et ses différents partenaires, selon que l'ETNIC soit sous-traitant au sens de l'article 4(8) du RGPD, responsable de traitement ou responsable de traitement conjoint au sens de l'article 4(7) du RGPD. Comme l'indique le demandeur, l'avant-projet de décret a principalement pour but de répondre aux exigences de l'article 28 du RGPD.

II. EXAMEN DE LA DEMANDE D'AVIS

Contexte

3. Le demandeur indique dans l'exposé des motifs de l'avant-projet de décret que : « *si l'effet direct du RGPD en droit belge rend directement applicable les dispositions qui régissent la sous-traitance, afin de respecter l'obligation formelle contenue à l'article 28, §3 du RGPD, il apparait nécessaire de reprendre la teneur de certaines dispositions dans un décret. A défaut, ces dispositions devraient chaque fois être reprises dans une convention à conclure avec chaque bénéficiaire, avec le risque qu'aucune convention ne soit jamais signée sur le sujet* ». L'Autorité rappelle conformément à la jurisprudence de la Cour de Justice de l'Union Européenne que l'applicabilité directe des règlements européens emporte l'interdiction de la retranscription dans le droit interne des dispositions des Règlements car un tel procédé peut « *(créer) une équivoque en ce qui concerne tant la nature juridique des dispositions applicables que le moment de leur entrée en vigueur* »[1].

4. L'Autorité souhaite aussi souligner que la volonté du demandeur d'intégrer les dispositions de l'article 28 du RGPD dans un texte législatif semble contradictoire avec le souhait de « *mettre*

[1] CJUE, 7 février 1973, Commission c. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Voir, également et notamment, CJUE, 10 octobre 1973, Fratelli Variola S.p.A. c. Administration des finances italienne (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11 ; CJUE, 31 janvier 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99**,** §§ 24-26.

en place un instrument dynamique et facilement modifiable » comme le stipule l'article 4 de de l'avant-projet de décret (commentaires des articles). En effet, l'avis de l'Autorité devra être sollicité à chaque modification des dispositions contenues dans l'avant-projet de décret conformément à l'article 23(1) de la LCA. Le demandeur aurait pu faire le choix d'adopter une convention cadre adjointe aux contrats conclus avec ses « bénéficiaires » sans figer ces dispositions dans la loi au risque de contrevenir aux dispositions du Règlement et aux futures positions du Comité Européen de la Protection des Données.

5. Enfin, l'Autorité souhaite souligner le risque que les clauses ne soient pas appropriées aux bénéficiaires des services de l'ETNIC ou dans les cas où l'ETNIC est un responsable de traitement, à la relation de l'ETNIC avec un sous-traitant en contradiction avec l'article 4(8) du décret ETNIC qui stipule que la convention cadre entre l'ETNIC et chaque bénéficiaire doit fixer les modalités d'organisation spécifiques à un bénéficiaire en matière de traitement des données à caractère personnel en application du RGPD.

Commentaire par article

Article 1er

6. L'article 1er (7) de l'avant-projet de décret définit l'Autorité de contrôle comme « *l'Autorité de Protection des Données (APD), instituée par la loi du 3 décembre 2017 portant sa création, et/ou toute autre autorité publique indépendante qui serait instituée au niveau communautaire pour surveiller l'application du RGPD et qui serait compétente pour contrôler les opérations de traitement effectuées par le bénéficiaire et/ou l'ETNIC* » (souligné par l'Autorité). Actuellement, une telle Autorité instaurée au niveau communautaire n'existe pas, dès lors, nous suggérons de ne pas définir l'Autorité de contrôle et de se référer à l' « Autorité de contrôle compétente ».

Article 3

7. L'article 3(2) de l'avant-projet de décret stipule que « *sauf accord contraire prévu dans la convention-cadre, chacun est responsable de respecter les obligations découlant du RGPD* ». La hiérarchie des normes impose évidemment la primeur du RGPD sur la convention cadre dès lors un accord contraire au RGPD serait nul et non avenu. De plus cet article indique que « *les articles du chapitre III du présent décret sont également applicables lorsque l'ETNIC intervient en qualité de responsable de traitement conjoint du traitement au côté d'un bénéficiaire* », alors que le chapitre III traite de la sous-traitance. Il est nécessaire d'opérer une distinction claire entre « sous-traitance » et « responsabilité conjointe ».

Article 4

8. L'avant-projet de décret stipule en son article 4 que « *les traitements de données à caractère personnel qui sont confiés en sous-traitance par le bénéficiaire à l'ETNIC sont ceux qui sont nécessaires à la réalisation des activités, projets et services confiés par le bénéficiaire à l'ETNIC, tels que repris dans les fiches visées à l'article 4, §3 du décret du 25 octobre 2018 relatif à l'Entreprise publique des Technologies Numériques de l'Information et de la Communication de la Communauté française. Ces traitements sont identifiés et détaillés dans les fiches susvisées annexées à la convention-cadre et modifiées selon les modalités définies par cette dernière* » (souligné par l'Autorité). Ces fiches sont définies par l'article 4§3 du décret ETNIC comme suit : « *en annexe à la convention cadre visée au paragraphe 1, est reprise, sous forme de fiches, la liste des activités, projets et services réalisés par l'ETNIC pour le bénéficiaire, qui contient au minimum le périmètre, les ressources humaines et financières, la durée ainsi qu'une projection budgétaire pluriannuelle* ». L'article 28(3) du RGPD impose que les mentions obligatoires figurent dans le contrat ou l'acte juridique lui-même et non pas dans des annexes ou listes dont la valeur juridique n'est pas connue. Cette exigence stricte permet d'assurer la sécurité juridique et la transparence des engagements pris entre responsables de traitement et sous-traitants.

9. Entre autres, les obligations et droits du responsable de traitement sont manquantes dans l'énumération des mentions obligatoires qui doivent figurer dans les listes. Il est indispensable que toutes les mentions de l'article 28(3) du RGPD soient inclues dans le contrat entre le sous-traitant et le responsable de traitement.

Article 5

10. L'Autorité prend acte de la disposition mais rappelle que la détermination des rôles de responsable de traitement, sous-traitant et responsable de traitement conjoint est factuelle[2], et que conformément à l'article 28(10) du RGPD si l'ETNIC outrepasse son rôle en tant que sous-traitant, elle sera requalifiée comme responsable de traitement en dépit de la qualification juridique de l'ETNIC en tant que sous-traitant.

[2]WP169https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2010/wp169_en.pdf, p. 9

Article 7

11. L'article 7§4 de l'avant-projet de décret prévoit que « *Si l'ETNIC estime qu'une des instructions qui lui est donnée par le bénéficiaire viole la réglementation en vigueur applicable en matière de protection des données à caractère personnel, elle a le devoir de le signaler immédiatement au bénéficiaire ainsi qu'à son délégué à la protection des données. L'ETNIC ne procède au traitement que si le bénéficiaire lui confirme, par écrit, l'instruction donnée. En tout état de cause, l'ETNIC ne peut pas être tenue pour responsable des conséquences d'une instruction qui violerait la réglementation et qu'elle n'aurait pas pu raisonnablement découvrir*». Cette disposition enfreint le prescrit de l'article 82(2) du RGPD qui stipule qu' « *un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci ».* L'avant-projet de décret ne peut prévoir un régime de responsabilité différent de celui prévu par le RGPD en exonérant le sous-traitant de sa responsabilité si le sous-traitant exécute une instruction illicite du responsable de traitement.

Article 8

12. L'Autorité formule la même recommandations qu'au point 8 concernant l'article 4 de l'avant-projet de décret. Tant la durée nécessaire à l'exécution des missions de sous-traitance pour lesquelles les données sont mises à disposition de l'ETNIC, que le choix du responsable de traitement à l'issue de la prestation de services de supprimer toutes les données personnelles ou de les renvoyer au bénéficiaire doivent être repris dans la convention elle-même.

Article 9

13. L'article 9§2 de l'avant-projet de décret stipule que la communication de données à caractère personnel à des tiers, de quelque manière que ce soit, est interdite, à moins qu'une disposition légale ou décrétale ou une injonction émise par un tribunal ou un organisme gouvernemental compétent oblige l'ETNIC à les communiquer. Il est indispensable de préciser dans l'avant-projet ce que le demandeur entend par « *injonction émise par un organisme gouvernemental compétent* ».

Article 10

14. Le paragraphe premier de l'article 10 énonce que sans préjudice de l'article 20 de l'avant-projet de décret, l'ETNIC ne peut transférer de données personnelles en dehors de l'Espace économique européen sauf instruction préalable du bénéficiaire. L'exception à cette règle de l'article 20 stipule que : « *l'ETNIC est autorisée à sous-traiter tout ou partie du traitement des données à un sous-traitant consécutif, en ce compris si cela entraine un transfert des données en dehors de l'Union européenne et de l'Espace Économique Européen, pour autant que le pays tiers dans lequel les données sont transférées offre un niveau de protection approprié par le biais d'une décision d'adéquation de la Commission européenne en vertu de l'article 45, paragraphe 3 du RGPD, ou que ce transfert soit encadré par des garanties appropriées en vertu de l'article 46 du RGPD* » (souligné par l'Autorité). Conformément au prescrit de l'article 28(3)(a) du RGPD, la décision de transférer des données en dehors de l'Espace économique européen y compris par le biais d'un sous-sous-traitant est une prérogative qui relève uniquement du responsable de traitement et le sous-traitant ne peut s'arroger le droit de transférer des données en dehors de l'EEE comme le prévoit l'article 20 de l'avant-projet de décret.

Article 14

15. L'article 14§3 de l'avant-projet de décret stipule que : « *sans préjudice du paragraphe 1er, dans toute la mesure du possible et en tenant compte de la nature du traitement, l'ETNIC aide le bénéficiaire, par des mesures techniques et organisationnelles appropriées, à s'acquitter de ses obligations de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits* » (souligné par l'Autorité). L'obligation de mettre en place des mesures de sécurité conformément à l'article 28(3)(c) est une obligation de résultat et non pas de moyen et l'Autorité recommande d'éviter l'ajout de la formulation telle que « *dans toute la mesure du possible »* qui en plus d'être vague, limite potentiellement l'étendue des obligations du sous-traitant au risque d'enfreindre l'article 28 du RGPD.

16. L'article 14§3 de l'avant-projet de décret ne reflète que le prescrit de l'article 28(3)(c) du RGPD or, il est indispensable d'inclure les autres obligations du sous-traitant en prévoyant conformément à l'article 28(3)(f) du RGPD que le sous-traitant aide le responsable de traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD.

Article 17

17. L'article 17§4 de l'avant-projet de décret indique que : « **«** *si le bénéficiaire le juge nécessaire, il informe les personnes concernées et les tiers, y compris l'autorité de contrôle, de toute violation de données »* (souligné par l'Autorité). La formulation actuelle de cette obligation ne reflète pas les exigences du RGPD qui prévoient une notification ou/et une communication à l'autorité de contrôle et aux personnes concernées dans les cas précis listés aux article 33 et 34 du RGPD.

Article 19

18. L'article 19 de l'avant-projet de décret stipule que : « *le bénéficiaire dispose du droit de procéder à toute vérification qui lui paraît utile pour constater le respect par l'ETNIC de ses obligations à l'égard des traitements pour lesquels elle agit en qualité de sous-traitant. Ce droit comprend le droit d'auditer les pratiques de sécurité de l'ETNIC relativement aux données à caractère personnel […] §3. Ces audits sont réalisés à un moment convenu conjointement entre le bénéficiaire et l'ETNIC ou à d'autres moments jugés nécessaires par le bénéficiaire à la suite d'une violation de données, ou à un soupçon de cet ordre»* (souligné par l'Autorité). Ces dispositions sont trop limitatives car les mesures d'audit qui peuvent être requises par le responsable de traitement ne se limitent pas aux mesures de sécurité et ne peuvent pas être circonscrites aux cas de violation de données ou « soupçon de cet ordre » par rapport au prescrit de l'article 28(3)(h) du RGPD.

Article 20

19. L'article 20 de l'avant-projet de décret autorise l'ETNIC à sous-traiter tout ou partie du traitement des données à un sous-traitant consécutif. L'Autorité constate que le législateur prive ce faisant le responsable de traitement de son droit conformément à l'article 28.2 du RGPD de choisir si son sous-traitant peut ou non sous-traiter le traitement de données dont il est responsable à un autre sous-traitant. Cette disposition qui enlève toute marge de manœuvre au responsable de traitement contredit la logique de l'article 28 du RGPD qui consiste à permettre au responsable de traitement de garder la maitrise du traitement dont il est responsable.

20. Le commentaire de l'article 20 de l'avant-projet de décret indique que : « *le sous-traitant doit informer le responsable du traitement de tout ajout, suppression ou changement de sous-traitant ultérieur pour que le bénéficiaire puisse éventuellement s'y opposer pour des motifs légitimes*, que « la convention-cadre modalisera le droit de « veto » du bénéficiaire (les motifs valables du droit d'objection ne sont pas précisés par le RGPD) » et l'article 20 précise que

« *le bénéficiaire dispose du délai tel que fixé par la convention-cadre pour présenter ses objections. La sous-traitance consécutive ne peut être effectuée que si le bénéficiaire n'a pas émis d'objection pendant le délai susmentionné* » (souligné par l'Autorité). Ces dispositions sont trop limitatives par rapport au prescrit de l'article 28.2 RGPD qui ne prévoit pas d'obligation de motivation au refus de sous-traitance consécutive dans le chef du responsable de traitement ni un système de consentement tacite à la sous-traitance consécutive en l'absence de réponse du bénéficiaire.

Article 21

21. L'article 21 de l'avant-projet de décret stipule que lorsque l'ETNIC fait appel à un sous-traitant consécutif pour mener des activités spécifiques pour le compte du bénéficiaire, elle conclut avec lui un accord écrit qui lui impose des engagements « *au moins aussi contraignants que ceux qui découlent du présent décret, de ses éventuels arrêtés d'exécution et de la convention-cadre, en ce compris ses annexes* » (souligné par l'Autorité). Cette disposition n'est pas assez fidèle au texte de l'article 28.4 du RGPD qui impose que « les même obligations » que celles fixées dans le contrat entre le responsable de traitement et le sous-traitants sont imposées au sous-traitant consécutif par contrat.

PAR CES MOTIFS,

L'Autorité requiert que le demandeur tienne compte dans l'avant-projet de décret *relatif aux traitements de données à caractère personnel réalisés par l'entreprise publique des technologies numériques de l'information et de la communication de la communauté française (ETNIC) ou confiés par ses bénéficiaires* des remarques suivantes :

- Les dispositions du RGPD ne peuvent pas être reprises dans la législation nationale ;
- **Points 6, 7, 13, 15, 17, 21** - Une clarification et le cas échéant une reformulation des points soulevés est nécessaire ;
- **Points 8, 9, 12, 16** - L'article 28(3) du RGPD impose que toutes les mentions obligatoires figurent dans le contrat ou l'acte juridique lui-même et non pas dans des annexes à celui-ci ;
- **Point 11** - L'avant-projet de décret ne peut prévoir un régime de responsabilité différent de celui prévu par le RGPD en exonérant le sous-traitant de sa responsabilité si le sous-traitant exécute une instruction illicite du responsable de traitement ;
- **Point 14** - Conformément au prescrit de l'article 28(3)(a) du RGPD, la décision de transférer des données en dehors de l'Espace économique européen y compris par le biais d'un sous-sous-traitant est une prérogative qui relève uniquement du responsable de traitement et le

sous-traitant ne peut s'arroger le droit de transférer des données en dehors de l'EEE comme le prévoit l'article 20 de l'avant-projet de décret ;

- **Point 18** - Ces dispositions sont trop limitatives car les mesures d'audit qui peuvent être requises par le responsable de traitement ne se limitent pas aux mesures de sécurité et ne peuvent pas être circonscrites aux cas de violation de données ou « soupçon de cet ordre » par rapport au prescrit de l'article 28(3)(h) du RGPD ;
- **Point 19** - Le législateur ne peut priver le responsable de traitement de son droit conformément à l'article 28.2 du RGPD de choisir si son sous-traitant peut ou non sous-traiter le traitement de données dont il est responsable à un autre sous-traitant
- **Point 20** - Ces dispositions sont trop limitatives par rapport au prescrit de l'article 28.2 RGPD qui ne prévoit pas d'obligation de motivation au refus de sous-traitance consécutive dans le chef du responsable de traitement ni un système de consentement tacite à la sous-traitance consécutive en l'absence de réponse du bénéficiaire.

(sé) An Machtens
Administrateur f.f.

(sé) Willem Debeuckelaere
Président,
Directeur du Centre de connaissances