Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 60/2021 du 23 avril 2021

Objet : Avis sur l'avant-projet de loi relatif à l'initiative citoyenne européenne, au sens du Règlement européen (UE) n°2019/788 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'initiative citoyenne européenne (CO-A-2021-041)

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 « 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 de la Ministre de l'Intérieur, Annelies Verlinden, reçue le 25 février 2021 ;

Vu les informations complémentaires reçues en date du 22 mars 2021 ;

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

Émet, le 23 avril 2021, l'avis suivant :

I. Objet et contexte de la demande

1. En date du 25 février dernier, la Ministre de l'Intérieur a sollicité l'avis de l'Autorité sur l'avant-projet de loi relatif à l'initiative citoyenne européenne, au sens du Règlement européen (UE) n°2019/788 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'initiative citoyenne européenne (ci-après « l'avant-projet de loi »).

2. Ainsi que le relève l'exposé des motifs, une initiative citoyenne est un instrument de démocratie participative qui donne aux citoyens de l'Union la possibilité de s'adresser directement à la Commission pour lui présenter une demande l'invitant à soumettre une proposition d'action juridique. Selon l'article 3 du Règlement européen précité 2019/788, une telle initiative n'est valable que si elle a recueilli le soutien d'au moins un million de citoyens de l'Union européenne d'au moins un quart des Etats membres.

3. Les modalités des traitements de données à caractère personnel figurant dans les déclarations de soutien aux initiatives citoyennes sont encadrées par ce Règlement européen précité 2019/788.

4. L'avant-projet de loi soumis pour avis vise à adapter la législation nationale en la matière à la suite des modifications apportées par ce Règlement européen qui a abrogé le précédent Règlement (UE) 2011/211. Selon l'exposé des motifs de l'avant-projet de loi, ce nouveau Règlement implique les adaptations suivantes dans notre droit national : établissement d'un point de contact destiné à informer et assister gratuitement les groupes d'organisateurs et veiller à ce que les citoyens puissent soutenir des initiatives en ligne en utilisant des moyens d'identification électroniques notifiés ou en signant la déclaration de soutien avec une signature électronique au sens du Règlement eIDAS.

II. Examen

5. Tout en ne pouvant anticiper sur quels sujets porteront les initiatives européennes, il est probable que les déclarations de soutien signées pourront révéler des catégories particulières de données (au sens de l'article 9 du RGPD) concernant leurs signataires telles que leurs opinions politiques. Il importe que des garanties soient prévues pour encadrer adéquatement les traitements de données à caractère personnel qui ont lieu dans le cadre de l'organisation d'une initiative citoyenne et de se prémunir contre tout détournement de finalité en la matière.

6. A cet égard, l'Autorité relève que le Règlement (UE) précité 2019/788 encadre déjà les traitements de données qui sont réalisés dans ce cadre conformément aux critères usuels de qualité des normes qui encadrent des traitements de données à caractère personnel.

Assimilation de la mention du numéro d'identification du Registre national à la signature électronique

7. L'article 3, al. 2 de l'avant-projet de loi prévoit l'utilisation du numéro de Registre national dans le cadre de la collecte des données concernant les signataires des déclarations de soutien à une initiative citoyenne en ces termes : *« lorsque les citoyens soutiennent une initiative citoyenne en ligne par le biais du système central de collecte en ligne visé à 'article 10 du Règlement, ils peuvent signer une déclaration de soutien soit en utilisant la carte d'identité électronique, soit en mentionnant leur nom et leur numéro de Registre national*. ».

8. Ce faisant, l'avant-projet de loi tente d'exécuter l'article 10 du Règlement précité 2019/788 qui prévoit que « les Etats membres veillent à ce que les citoyens puissent soutenir les déclarations de soutien en utilisant des moyens d'identification électronique notifiés[1] ou en signant avec une signature électronique au sens du règlement européen (UE) n°910/2014.

9. Selon l'article 3.10 du Règlement eIDAS, une signature électronique est définie comme des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer.

10. Etant donné que l'on peut difficilement considérer qu'une personne utilise son numéro de Registre national pour signer un document, cette assimilation qui est faite à l'article 3, al. 2 de l'avant-projet de loi n'apparait pas conforme à la définition de la notion de signature électronique donnée par le Règlement eIDAS. Il convient donc de revoir le libellé de l'article 3, al. 2 en conséquence d'autant plus que cette assimilation n'est pas nécessaire au vu du choix de la Belgique d'imposer l'usage du formulaire de déclaration de soutien avec mention obligatoire du numéro d'identification du Registre national des signataires (cf. infra). Afin de se prémunir contre les fraudes à l'identité et afin d'éviter toute remise en cause du caractère authentique des signatures électroniques utilisées par les signataires des déclarations de soutien, l'Autorité recommande à l'auteur du projet de réaliser une analyse de risque pour évaluer quelle niveau de signature est requis en l'espèce[2].

---

[1] Soit la carte d'identité électronique belge selon la notification publiée le 27 décembre 2018 au journal officiel de l'Union européenne.

[2] A ce sujet il est renvoyé au guide du SPF Economie à destination des rédacteurs de textes législatifs et réglementaires relatif à l'utilisation des notions de « signature électronique » et autres « services de confiance » ainsi que de « support durable », disponible sur le site web à l'adresse suivante https://economie.fgov.be/sites/default/files/Files/Publications/files/Digital-Act-II-Guide-terminologique.pdf

L'Autorité recommande que soit imposé par l'avant-projet de loi, pour toutes les signatures électroniques des déclarations de soutien, au minimum l'usage d'une signature avancée au sens de l'article 3.11 du Règlement eIDAS.

Traitement du numéro d'identification du Registre national par la DG Institutions et Population du SPF Intérieur, les organisateurs et la Commission européenne

11. Quant à l'utilisation du numéro d'identification du Registre national dans ce cadre, l'Autorité rappelle que les numéros d'identification unique font l'objet d'une protection particulière. L'article 87 du RGPD prévoit que les Etats membres adoptant un numéro d'identification national doivent veiller à ce qu'il ne soit utilisé que sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Ajouter la mention du numéro du Registre national aux déclarations de soutien pouvant contenir des informations sensibles sur leurs signataires n'est pas sans risque au vu de la facilitation d'interconnexion de données que ce numéro permet. Si, ainsi qu'il ressort des informations complémentaires, la Belgique a posé ce choix (formulaire B de déclaration de soutien visé à l'annexe III du Règlement précité 2019/788 prévoyant la collecte du numéro d'identification du Registre national), il importe de le prévoir explicitement dans l'avant-projet de loi et que des garanties particulières soient prévues.

12. A cet égard, l'Autorité relève que l'article 19 du Règlement précité 2019/788 impose aux groupes d'organisateurs, à la Commission européenne ainsi qu'au service compétent du SPF Intérieur la destruction des déclarations et copies de déclaration de soutien signées au plus tard ; soit, dans le chef des organisateurs et de la Commission, un mois après la présentation de l'initiative à la Commission ou 21 mois après le début de la période de collecte ou encore un mois après le retrait de l'initiative, soit, dans le chef des services compétents du SPF Intérieur, trois mois après avoir émis le certificat établissant le nombre de déclarations de soutien valables.

13. Afin d'encadrer adéquatement l'utilisation de ce numéro, l'Autorité considère qu'il importe que l'avant-projet de loi précise clairement la ou les finalités pour lesquelles le numéro d'identification du Registre national sera utilisé dans ce cadre. Si, comme il ressort des informations complémentaires et du formulaire de demande d'avis, l'intention de l'auteur de l'avant-projet de loi est d'assurer que le numéro d'identification du Registre national de la personne qui signe la déclaration de soutien y soit mentionné et ce, pour que seuls les services compétents du SPF Intérieur puissent utiliser ce numéro pour consulter les données des signataires dans le Registre national nécessaires à la vérification de la validité des déclarations de soutien; il convient de préciser cet usage exclusif et cette finalité dans l'avant-projet de loi.

14. Par ailleurs, le traitement qui sera fait de ce numéro par l'organisateur d'une initiative citoyenne ou par la Commission européenne[3] (a priori simple conservation pendant les délais visés au Règlement précité 2019/788 sans aucune autre utilisation) sera utilement précisé dans l'avant-projet de loi.

15. Enfin, l'avant-projet de loi imposera utilement que le système particulier de collecte en ligne des déclarations de soutien garantira que le numéro d'identification du Registre national d'un signataire ne soit pas accessible aux autres signataires de la déclaration de soutien.

Vérification de la validité des déclarations de soutien par le SPF Intérieur

16. L'article 5 de l'avant-projet de loi prévoit les traitements de données à caractère personnel qui seront réalisés par les services compétents du SPF Intérieur pour vérifier la validité des déclarations de soutien signées par les ressortissants belges au regard du Règlement précité 2019/788 et ce en exécution de l'article 12 dudit Règlement.

17. A cet égard, l'Autorité s'interroge quant à la nécessité pour les services de la DG Institutions et Population
    - de vérifier la capacité juridique des signataires de déclarations de soutien à une initiative citoyenne européenne étant donné que cette vérification n'apparait pas requise à la lecture du Règlement précité 2019/788 et qu'une telle déclaration de soutien ne constitue pas un engagement juridique nécessitant d'avoir la capacité juridique pour le signer. L'article 2.2 du Règlement précité 2019/788 prévoit d'ailleurs explicitement que les Etats membres et la Commission européenne veillent à ce que les personnes atteintes d'un handicap puissent exercer leur droit de soutenir des initiatives. L'Autorité considère donc qu'il convient de supprimer l'article 5, §2, 3ème tiret et en conséquence l'autorisation d'accès à la donnée visée à l'article 3, alinéa 1er, 9°/1[4] de la loi du 8 août 1983 organisant un Registre national des personnes physiques (ci-après LRN).
    - de consulter l'adresse de résidence principale des signataires des déclarations de soutien : selon l'article 2 du Règlement précité 2019/788, le soutien à une initiative citoyenne est ouvert à tout citoyen de l'Union peu importe son lieu de résidence et selon l'article 12 de ce Règlement, le champ d'application *rationae personae* de la mission de vérification des déclarations de soutien de la DG Institutions et Population du SPF Intérieur est limité aux

[3] L'article 10 du Règlement précité de 2019 prévoit que les données obtenues au moyen du système central de collecte en ligne sont stockées sur les serveurs mis à disposition par la Commission européenne à cet effet. Il est également prévu que les organisateurs pourront télécharger les déclarations de soutien signées sur papier.

[4] A savoir « *les actes et décisions relatifs à la capacité juridique et les décisions d'administration de biens ou de la personne visées à l'[6 article 1250]6, alinéa 1er, du Code judiciaire; le nom, le prénom et l'adresse de la personne qui représente ou assiste un mineur, un interdit, un interné ou une personne placée sous statut de minorité prolongée, ou de l'administrateur de biens ou de la personne dont il est fait mention dans la décision visée à l'[6 article 1250]6, alinéa 1er, du Code judiciaire* ».

ressortissants belges sans égard à leur résidence. Par conséquent, à défaut de justification pertinente à ce sujet dans l'exposé des motifs, l'accès conféré à la DG Institutions et Population à la donnée visée à l'article 3, alinéa 1er, 5° de la LRN sera supprimé.

Sécurisation des systèmes particuliers de collecte en ligne utilisés par les organisateurs d'une initiative européenne

18. En ce qui concerne la sécurisation des systèmes particuliers de collecte en ligne utilisés par les organisateurs d'une initiative européenne qui peuvent être utilisés jusqu'au 31 décembre 2022, en lieu et place du système central de collecte en ligne mis à disposition par la Commission européenne, l'article 4 de l'avant-projet de loi impose au délégué à la protection des données des organisateurs d'une initiative européenne d'adresser aux services compétents du SPF Intérieur un engagement écrit par lequel les organisateurs attestent que leur système particulier de collecte est « *doté de dispositifs de sécurité et techniques adéquats permettant de rencontrer les exigences fixées à l'article 11, §3 et 4, à l'article 12, §2 et à l'article 18, 3 du Règlement précité de 2019 et que les données à caractère personnel sont traitées conformément au RGPD* ».

19. Tout d'abord, l'Autorité relève qu'imposer cette obligation au délégué à la protection des données (DPD) n'est pas compatible avec ses missions lui incombant en vertu de l'article 39 du RGPD. L'autonomie des DPD ne signifie pas qu'ils disposent de pouvoirs de décision allant au-delà des missions leur incombant conformément à l'article 39[5]. Si des engagements doivent être adressés aux services compétents du SPF Intérieur dans le cadre de la certification de leur système particulier de collecte de déclarations de soutien en ligne, c'est aux organisateurs eux-mêmes qu'il convient de les imposer. Comme cela a déjà été mis en évidence par le Comité européen à la protection des données dans ses lignes directrices concernant les délégués à la protection des données adoptées le 5 avril 2007[6], bien que l'exercice par le délégué à la protection des données de ses missions facilite la mise en conformité au RGPD (accountability), c'est le responsable de traitement et le cas échéant son sous-traitant qui demeurent en charge de la conformité à la règlementation en matière de protection des données et qui doivent être en mesure de démontrer que le traitement est effectué conformément au RGPD. Le délégué n'est pas personnellement responsable de cette conformité

20. Ensuite, l'engagement de traiter les données conformément au RGPD est superfétatoire, le RGPD étant d'application directe. De plus, c'est le Règlement précité de 2019 qui encadre spécifiquement les traitements de données à caractère personnel qui seront réalisés tant par les organisateurs, la

[5] Lignes directrices du G 29(n°16/FR WP 243 rev.0) concernant les délégués à la protection des données (DPD) adoptées le 5 avril 2017, p. 18, disponibles à ce sujet sur le site web de l'EDPB à l'adresse suivante

[6] Disponibles à l'adresse suivante https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Commission européenne que les autorités nationales compétentes en charge de la vérification et de la certification des déclarations de soutien.

21. Enfin, l'Autorité relève que
    - l'article 11, §3 du Règlement précité 2019/788 impose aux autorités de contrôle, à savoir la DG Institutions et Population du SPF Intérieur, de certifier la conformité du système particulier de collecte en ligne (dont les données sont stockées sur le territoire de la Belgique) aux exigences du paragraphe 4 de cet article 11 ; ce qui implique de vérifier que ce système est *« doté de dispositifs de sécurité et techniques adéquats pour garantir tout au long de la période de collecte que :*
        i. seules des personnes physiques peuvent signer une déclaration de soutien ;
        ii. les informations fournies sur l'initiative correspondent aux informations publiées dans le registre ;
        iii. les données sont collectées auprès des signataires conformément à l'annexe III (du règlement précité de 2019) *;*
        iv. *les données fournies par les signataires sont collectées et stockées d'une manière sécurisée* ».
    - et que, en exécution de l'article 11, § 5 de ce Règlement précité 2019/788, le Règlement d'exécution (UE) 2019/1799 de la Commission du 22 octobre 2019[7] encadre ces spécifications techniques. En plus de la désignation obligatoire d'un responsable de la sécurité par le groupe d'organisateurs, il est prévu que l'autorité compétente, à savoir la DG Institution et Population du SPF Intérieur, fournit à ces organisateurs les règles et exigences de sécurité pour la certification du système particulier de collecte, lesquelles portent sur les risques liés à la confidentialité et à l'intégrité des informations contenues dans le système (procédures de gestion des risques visées au point 4.2 de l'annexe à ce Règlement d'exécution 2019/1799) et tiennent compte des spécifications visées au point 4.3 de cette annexe en matière de cryptage des données.

22. Par conséquent, l'Autorité considère que l'article 4 de l'avant-projet de loi ne présente pas de plus-value par rapport à ces dispositions légales directement applicables. Seul le paragraphe 3 de l'article 4 de l'avant-projet de loi qui octroie aux services de la DG Institutions et Population le pouvoir de demander aux organisateurs de leur communiquer les documents nécessaires pour vérifier si le système est doté de dispositifs de sécurité et techniques adéquats sera préservé en adaptant toutefois sa formulation de manière telle que la demande d'information doive être adressée aux organisateurs et non au délégué à la protection des données (cf. supra).

[7] Règlement d'exécution (UE) 2019/1799 de la Commission du 22 octobre 2019 établissant des spécifications techniques pour les systèmes particuliers de collecte en ligne conformément au règlement (UE) 2019/788 du Parlement européen et du Conseil relatif à l'initiative citoyenne européenne.

Par ces motifs,

L'Autorité

considère que l'avant-projet de loi soumis pour avis doit être adapté en ce sens :

1. Suppression de l'assimilation de la mention du numéro d'identification du Registre national à la signature électronique et imposition de l'usage au minimum de signatures électroniques avancées (cons. 9 et 10) ;
2. Détermination dans l'avant-projet de loi du choix de la Belgique d'opter pour le modèle B de formulaire de déclaration de soutien visé à l'annexe III du Règlement précité (cons. 11) ;
3. Mention plus explicite de la finalité concrète pour laquelle la DG Institutions et Population utilisera ce numéro dans sa mission de vérification et certification des déclarations de soutien et du traitement de simple conservation sécurisée pendant le temps nécessaire qui sera fait de ce numéro pour les organisateurs d'initiative européenne et la Commission européenne (cons. 13 à 15) ;
4. Suppression de la vérification de la capacité juridique et de la résidence dans l'Union européenne des signataires des déclarations de soutien par la DG Institutions et Population et adaptation en conséquence de la liste des données du Registre national auxquelles un accès lui est conféré dans ce cadre (cons. 17) ;
5. Suppression des paragraphes 1 et 2 de l'article 4 de l'avant-projet de loi (cons. 18 à 22).

Rappelle que c'est le responsable de traitement et le cas échéant son sous-traitant qui demeurent en charge de la conformité à la règlementation en matière de protection des données et qui doivent être mesure de démontrer que le traitement est effectué conformément au RGPD. Le délégué à la protection des données n'est pas personnellement responsable de cette conformité bien que l'exercice de sa mission y participe (cons. 19).

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances