Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 144/2023 du 29 septembre 2023

Objet: Demande d'avis concernant un avant-projet de loi modifiant la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public (CO-A-2023-334)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

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 l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

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 Secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée et de la Régie des bâtiments, Monsieur Mathieu Michel (ci-après « le Secrétaire d'Etat »), reçue le 12 juillet 2023 ;

Émet, le 29 septembre 2023, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. Le Secrétaire d'Etat a introduit auprès de l'Autorité une demande d'avis concernant les articles 2, 1° à 5° et 14° à 20°, 3, 6*bis*, 9, 10*bis*, 12*bis* à 15*bis* et 17*bis* d'un avant-projet de loi *modifiant la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public* (ci-après, « le Projet »). Ces dispositions, qui modifient la loi du 4 mai 2016 *relative à la réutilisation des informations du secteur public* (ci-après, « **la loi de 2016** »), transposent la Directive (UE) n° 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 *concernant les données ouvertes et la réutilisation des informations du secteur public (refonte)* (ci-après, « **la Directive** »).

II. Examen

2. L'Autorité s'est déjà prononcée à plusieurs reprises au sujet de la réutilisation des informations du secteur public et de la transposition de la Directive. **Elle renvoie à titre introductif, aux avis suivants dans lesquels sont rappelés les principes de protection des données appliqués au domaine de la réutilisation des informations du secteur public** :

   - Avis n° 203/2021 du 25 octobre 2021 *concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2021-196)* ;

   - Avis n° 167/2022 du 19 juillet 2022 *concernant un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public, et un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public pour les matières réglées à l'article 138 de la Constitution (CO-A-2022-150)* ;

   - Avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209).*

3. Parmi les modifications qu'il apporte à la loi de 2016, **le Projet s'aligne sur une récente réforme de la loi du 11 avril 1994 *relative à la publicité de l'administration*** (ci-après, « la **loi de 1994** »). L'autorité s'est prononcée à deux reprises au sujet de cette réforme et **renvoie par conséquent également, à titre introductif, à ces avis précédents** :

   - Avis n° 42/2023 du 9 février 2023 *concernant un avant-projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration (CO-A-2022-311)* ;

- Avis n° 131/2023 du 8 septembre 2023 *concernant un amendement n° 4 du projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration et abrogeant la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes (CO-A-2022-316)*.

II.1. Données à caractère personnel susceptibles de réutilisation

4. Sur le plan du principe, en ce qui concerne les données à caractère personnel qui sont susceptibles d'être accessibles à des fins de réutilisation, le Projet ne modifie pas les principes actuellement consacrés dans l'article 3, § 2, 4° et 5°, de la loi de 2016. Selon ces dispositions, la loi de 2016 ne s'applique pas aux « *documents administratifs qui conformément aux règles d'accès public en vigueur ne peuvent être rendus accessibles* »[1] et aux « *documents administratifs pour lesquels l'accès peut uniquement être obtenu en vertu des règles prévoyant un droit d'accès personnel ou un intérêt* » (souligné par l'Autorité)[2]. Il en découle que **des données à caractère personnel ne pourront être réutilisées que si l'accès à celles-ci est ouvert au grand public, sans nécessiter la justification d'un quelconque intérêt[3]**.

II.2. Instances publiques

[1] Le Projet ajoute à cette disposition la précision suivante : « *comme par exemple en raison de la protection de la sécurité de la population, la sûreté ou la défense nationale, la sécurité publique et l'ordre public dans le cadre existant de la législation sur la publicité de l'administration* ».

[2] Voir également plus explicitement, l'article 1er, 2., h) (comparer avec le f)) de la Directive.

L'exposé des motifs explique notamment ce qui suit :

« *Une exclusion importante, déjà incluse dans la loi existante du 4 mai 2016, sera évidemment maintenue et est applicable aux documents administratifs qui, sur base des règles de l'accès public en vigueur (c.à.d. les règlementations relatives à la publicité de l'administration), ne sont pas accessibles ou auxquels il est possible d'accéder uniquement sur la base d'un droit d'accès personnel ou d'un intérêt.*

Cette non-applicabilité de la loi vise, entre autres, les exclusions motivées par :

[…]

- *les libertés et les droits fondamentaux des administrés ;*

[…]

- *le caractère par nature confidentiel des informations d'entreprise ou de fabrication et des informations commerciales (secret des professionnel, secret d'affaires ou secret d'entreprise) communiquées à l'autorité ;*
- *le secret de l'identité de la personne qui a communiqué le document ou l'information à l'autorité administrative à titre confidentiel pour dénoncer un fait punissable ou supposé tel ;*
- *la protection de la vie privée ;*
- *la protection d' une obligation de secret instaurée par la loi, comme le secret statistique ;*
- […] ».

[3] A ce sujet, voir les considérants nos 4-12 de l'avis n° 203/2021 du 25 octobre 2021 *concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2021-196)*.

5. Dans la logique de la réforme précitée de la loi de 1994, le Projet remplace dans la loi de 2016, le concept d' « *autorité publique* » par celui d' « *instance publique* »[4], dont la définition est complétée par rapport au droit positif. L'exposé des motifs du Projet exprime en détails ce qui suit, à ce sujet :

> « *En conformité avec la modification à court terme de la loi du 11 avril 1994, le champ d'application ratione personae de la loi du 4 mai 2016 est également élargi, en ne le limitant plus aux autorités administratives visées à l'article 14 des lois coordonnées sur le Conseil d'Etat et telle que déterminée par la jurisprudence*[.] *Dorénavant, d'autres instances seront également soumises à la loi du 11 avril 1994 et à la loi du 4 mai 2016.*
>
> *Ainsi, le champ d'application de la loi comprend notamment :*
> - *les provinces et les communes, lorsqu'elles exercent des compétences fédérales ;*
> - *les organismes d'intérêt public, à savoir les organismes visés par l'article 1er de la loi du 16 mars 1954 relative au contrôle de certains organismes d'intérêt public, lorsqu'ils exercent des compétences fédérales ;*
> - *les zones de police pluricommunales visées par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et leurs organes, lorsqu'ils exercent des compétences fédérales ;*
> - *les zones de secours visées par la loi du 15 mai 2007 relative à la sécurité civile et leurs organes, lorsqu'ils exercent des compétences fédérales.*
>
> *En résumé, la nouvelle définition de l' 'instance publique' inclut donc, tout d'abord, toutes les entités énumérées à l'article 2, 1° en a) à d), qui étaient déjà dans le champ d'application de la loi du 4 mai 2016 en vertu du droit européen. De plus, les instances administratives qui ne tombaient pas encore dans le champ d'application actuel de la présente loi, tel que décrit ci-dessus, mais qui sont effectivement soumises aux règles de publicité de la loi du 11 avril 1994, sont désormais également incluses dans le champ d'application de la présente loi par l'insertion d'une nouvelle disposition à l'article 2,1° e) et f).*
>
> *Enfin, en conformité avec la modification à court terme de la loi du 11 avril 1994 relative à la publicité de l'administration, par l'insertion d'une nouvelle disposition à l'article 2, 1°, g) qui clarifie qu'aux fins de la présente loi, on entend également par 'Instance publique' : les organes stratégiques du gouvernement fédéral visés par l'arrêté royal du 19 juillet 2001 relatif à l'installation des organes stratégiques des services publics fédéraux et relatif aux membres*

[4] Dans son état au moment de la saisine de l'Autorité, le projet alors soumis pour avis consacrait désormais le concept d' « *instance administrative* » qui inclut notamment les autorités administratives au sens de l'article 14 des *lois coordonnées sur le Conseil d'Etat*, voir les considérants nos 4-6 de l'avis n° 42/2023 du 9 février 2023 *concernant un avant-projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration (CO-A-2022-311)*.

du personnel des services publics fédéraux désignés pour faire partie du cabinet d'un membre d'un Gouvernement ou d'un Collège d'une Communauté ou d'une Région.

On vise donc principalement ce que l'on appelle les cabinets ministériels et les cabinets des secrétaires d'État (étant entendu que la désignation officielle du cabinet est 'organe stratégique'). Il apparait de l'exposé des motifs accompagnant la modification à court terme de la loi du 11 avril 1994 relative à la publicité de l'administration, qu'il existe au moins un doute quant à la mesure dans laquelle ces instances sont soumises aux obligations de publicité de l'administration, telles que reprises au niveau fédéral dans la loi du 11 avril 1994.

C'est pourquoi la loi du 4 mai 2016, par analogie avec la législation sur la publicité de l'administration vise explicitement à intégrer les documents administratifs des organes stratégiques dans le champ d'application de la législation ».

6. Cette extension du champ d'application *ratione personae* de la loi de 2016 n'appelle pas plus de commentaires de la part de l'Autorité que n'en a appelé la réforme de la loi de 1994.

II.3. Application des règles de protection des données

7. L'article 3, § 3, en projet de la loi de 2016, prévoit l'application des règles de protection des données en ces termes :

« *La présente loi est sans préjudice des dispositions du droit de l'Union et du droit national relative à la protection des données à caractère personnel, en particulier 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/ ; la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, ainsi que des dispositions correspondantes du droit belge ; la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ; la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque carrefour de la sécurité sociale et les arrêtés d'exécution de ces lois.*

Des données à caractère personnel sont seulement réutilisables dans la mesure où cette réutilisation est conforme avec la législation concernant la protection des données à caractère personnel et avec la protection des droits et libertés des personnes concernées.

Les données à caractère personnel sont, le cas échéant, anonymisées ou pseudonymisées par l'instance publique, ou par un tiers de confiance pour le compte et sur instruction de l'instance publique, préalablement à la transmission en vue de leur réutilisation » (souligné par l'Autorité).

8. Au sujet de cette disposition, l'exposé des motifs développe notamment ce qui suit :

« *L'instance publique responsable doit évaluer dans chaque cas et de manière concrète si les conditions de l'article 6.4 du RGPD (analyse de compatibilité) sont remplies. La réutilisation proportionnée doit être accompagnée de conditions relatives au respect des règles de protection des données à caractère personnel.*

En principe, les données à caractère personnel ne peuvent être réutilisées qu'après avoir été rendues anonymes ou pseudonymisées. L'anonymisation ou la pseudonymisation des informations est un moyen de concilier l'intérêt de rendre les informations du secteur public aussi réutilisables que possible avec les obligations découlant de la règlementation sur la protection des données. […]

L'anonymisation ou la pseudonymisation doit être effectuée par l'institution publique responsable ou l'entreprise publique responsable avant que les données ne soient transférées pour être réutilisées. Cela peut impliquer l'intervention d'un tiers de confiance certifié qui effectue et garantit l'anonymisation ou la pseudonymisation de l'ensemble des données, aux frais de l'institution ou de l'entreprise publique. L'anonymisation et la pseudonymisation doivent être effectuées par l'instance publique ou l'entreprise publique préalablement au transfert des données en vue de leur réutilisation.

Le texte crée la possibilité de réutiliser des documents contenant des données à caractère personnel anonymisées ou pseudonymisées.

Le choix de l'anonymisation ou de la pseudonymisation doit être fait délibérément sur la base d'une analyse des circonstances concrètes de l'affaire, de la nature des données à caractère personnel et des catégories de personnes concernées, des finalités initiales pour lesquelles ces données ont été traitées, de la portée, du contexte et des objectifs de la réutilisation et du risque élevé ou non pour les droits et libertés des personnes physiques.

En ce qui concerne le choix de l'anonymisation ou de la pseudonymisation et en ce qui concerne les techniques et stratégies d'anonymisation ou de pseudonymisation à utiliser, on peut se référer, entre autres, à l'Avis no. 5/2014 sur les techniques d'anonymisation du 10

avril 2014, WP216 du « Groupe de travail Article 29 sur la protection des données « , les (futurs) travaux du Conseil européen de la protection des données (EDPB) et de l'ENISA, l'Agence de cybersécurité de l'Union européenne (« Rapport de l'ENISA sur la pseudonymisation des données : techniques avancées et cas d'utilisation, publié le 28 janvier 2021 et rapport de l'ENISA sur les meilleures pratiques et techniques de pseudonymisation » publié le 3 décembre 2019) dans ce domaine.

L'anonymisation ou la pseudonymisation doit tenir compte des risques potentiels de réidentification des données anonymes ou pseudonymisées et peut nécessiter la recommandation de mesures supplémentaires pour protéger au mieux la vie privée.

Une garantie supplémentaire pour les personnes concernées consiste à obtenir un avis de l'Autorité de protection des données sur le caractère approprié de la mesure dans ce cas particulier. L'Autorité de protection des données, qui dispose de l'expertise nécessaire en la matière, peut donner son avis sur le type et la force de la pseudonymisation et/ou le tiers de confiance certifié choisi, ou recommander l'anonymisation pour certaines catégories de données.

Ces dispositions s'appliquent sans préjudice des règles spécifiques au traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques prévues par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel » (souligné par l'Autorité).

9. Premièrement, l'Autorité est d'avis que dans la logique exprimée dans l'exposé des motifs, mais non retranscrite dans le dispositif du Projet, ce dernier doit, compte-tenu de la grande diversité des traitements envisagés, conformément au principe de minimisation des données consacré dans l'article 5, 1., c), du RGPD, **imposer à l'instance publique le recours à l'anonymisation des données avant d'en permettre réutilisation ou, à défaut, si l'anonymisation ne permet pas d'accomplir l'objectif escompté** (à savoir la finalité de la réutilisation envisagée) **et pour autant que cela soit proportionné dans le cas d'espèce, la pseudonymisation des données à caractère personnel avant de permettre leur réutilisation** (sachant que des données pseudonymisées restent des données à caractère personnel, ce qui limite leur utilisation).

10. Cela étant précisé, l'Autorité attire en outre l'attention du demandeur sur les **considérants nos 17-19 de son avis n° 203/2021** du 25 octobre 2021 *concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2021-196)*, selon lesquels :

« […] *il importe de souligner que l'état de la technique et les techniques d'anonymisation sont évolutives, tout comme les données disponibles (publiquement ou pas) qui rendraient les données identifiables du point de vue des destinataires des données dé-identifiées (p. ex., nouvelles possibilités de réidentification des personnes concernées lorsqu'il y a eu une fuite de données, publication d'autres jeux de données qui n'étaient pas encore disponibles au moment de l'anonymisation, etc.*[…]). *Dans un tel contexte, l'état anonyme ou non de données pourtant « anonymisées » et communiquées comme telles (à savoir, comme sortant du champ d'application du RGPD) variera avec le temps. De telle sorte qu'un traitement d'anonymisation des données à caractère personnel fondé sur la « dé-identification » des données (sur la base d'une des techniques renseignées plus haut – randomisation, etc.) qui sont ensuite communiquées comme telles aux demandeurs de réutilisations de données, pourrait amener le demandeur à partager des données qui deviendraient ré-identifiables sans que celui-ci ne puisse – a posteriori – limiter leur diffusion.*

En outre, ces techniques pourraient limiter (potentiellement trop strictement, selon la nature des données originales et compte-tenu de la finalité de la réutilisation concernée – ce qui est à étudier au cas par cas,) les possibilités de traitement (et partant l'utilité) des données « anonymisées » pour les demandeurs de réutilisation et la société dans son ensemble.

Partant, l'Autorité attire l'attention du demandeur sur ***d'autres possibilités techniques existantes qui pourraient également contribuer à la réutilisation des données concernées, le cas échéant de manière plus efficiente,*** *en maintenant des conditions techniques contraignantes quant à l'utilisation des données qui peut être envisagée par le demandeur et en organisant différemment (plutôt qu'une simple communication des données dé-identifiées) la manière dont les données sont mises à disposition des demandeurs, comme par exemple via des services*[5] » (mise en gras et souligné par l'Autorité dans le présent avis).

11. **Dans une perspective plus globale** dans le domaine de la réutilisation des informations du secteur public, **l'Autorité attire l'attention du demandeur sur l'importance de prendre en considération ce type d'autres possibilités**. Dans ces hypothèses, plutôt que de prévoir la communication de données à caractère personnel (brutes, pseudonymisées, ou la communication de données rendues anonymes) au demandeur qui entend réutiliser les données, des **services d'accès sécurisé aux données concernées** sont offerts par une entité tierce (qui peut être un tiers de confiance[6]), à ce demandeur. De cette manière, tant d'un point de vue normatif (le traitement de

[5] « *Voir par exemple https://www.casd.eu* », dernièrement consulté le 20/09/2023. Voir également K. GADOUCHE, « The Secure Data Access Centre (CASD), a Service for Datascience and Scientific Research », 22/06/2021, disponible sur https://www.insee.fr/en/information/5014754?sommaire=5014796, dernièrement consulté le 20/09/2023.

[6] Voir les considérants nos 13 et s. concernant le concept de « tiers de confiance » auquel recourt le Projet. Le prestataire de service concerné pourrait être considéré comme un tiers de confiance et devoir rencontrer les exigences applicables à ce type

données demeure soumis au RGPD) que technique, **un meilleur contrôle peut être garanti sur le traitement des données tout en permettant la réutilisation des données concernées**. De tels services pourraient ainsi contribuer à maximiser à la fois, les possibilités de réutilisation des données et les garanties pour les droits et libertés des personnes concernées.

12. En l'état de la technique, compte-tenu de la complexité liée à la mise en œuvre d'un processus optimal d'anonymisation des données au regard des risques de réidentification, **l'Autorité est d'avis qu'il convient de privilégier ce type de services d'accès aux données en vue de leur réutilisation**, plutôt que de prévoir la communication de jeux de données (pseudonymisées ou rendues anonymes), s'agissant d'une méthode plus efficace pour garantir à la fois le contrôle sur le traitement des données et des possibilités de réutilisation de celles-ci.

13. Deuxièmement, le Projet ne définit pas la notion de « ***tiers de confiance certifié*** », ni ne se réfère à un cadre normatif relatif à la certification dont il serait question. S'agissant du recours à un concept tel que celui de « *tiers de confiance* », au considérant n° 53 de son avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage' (CO-A-2022-003)*[7], l'Autorité a exprimé ce qui suit :

> « *Dans ce contexte, l'Autorité ne s'oppose pas à l'utilisation d'un « tiers de confiance » pour la réalisation de la pseudonymisation ou l'anonymisation des donnés. Cette notion n'existant pas dans le* [RGPD]*, le projet devra cependant définir ce que constitue un « tiers de confiance » dans le cadre de ce projet, et surtout, les responsabilités et qualités qui sont attendues de ce tiers par rapport par exemple à un sous-traitant. A titre d'exemple l'article 2, 3°, a), de l'accord de coopération attribue un rôle potentiellement similaire à la BCED*[8] *: « une entité indépendante de confiance qui offre des services qui accroissent la fiabilité de l'échange électronique de données et de l'enregistrement de données et qui n'a elle-même*

d'entité. Cela étant précisé, en l'état, le Projet ne permet l'intervention d'un tel tiers de confiance que pour procéder à l'anonymisation ou à la pseudonymisation des données. Concernant le CASD cité à la note de bas de page n° 5, l'Autorité relève néanmoins qu'il ne couvre pas toutes les hypothèses visées par la réutilisation des données au sens de la Directive et de la loi de 2016 dans la mesure où « *le CSAD a pour objet principal d'organiser et de mettre en œuvre des services d'accès sécurisé pour les données confidentielles à des fins non lucratives de recherche, d'étude, d'évaluation ou d'innovation. Il a également pour mission de valoriser la technologie développée pour sécuriser l'accès aux données dans le secteur public et dans le secteur privé* » (https://www.casd.eu/le-centre-dacces-securise-aux-donnees-casd/gouvernance-et-missions/, dernièrement consulté le 21/09/2023) (souligné par l'Autorité).

[7] La position suivante est également exprimée aux considérants nos 46-48 de son avis n° 143/2023 de l'Autorité du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376).*

[8] Soit la « Banque-Carrefour d'échanges de données » au sens de l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française *portant sur le développement d'une initiative en commun en matière de partage de données et sur la gestion conjointe de cette initiative*.

aucune mission ou aucun intérêt en matière de traitement réel de [fond] de données à caractère personnel » (souligné par l'Autorité). Compte-tenu de cette définition, l'article 106/20 en projet pourrait par exemple avoir comme objectif d'imposer le recours à une entité indépendante/neutre à l'égard des traitements envisagés et des responsables du traitements concernés, qui n'a pas d'intérêt à connaître les données à caractère personnel traitées ou le résultat de leur traitement, et qui dispose d'une expertise avérée, conforme à l'état de l'art en matière de traitement de données à caractère personnel et en particulier, de pseudonymisation et d'anonymisation de données à caractère personnel. A cet égard, dès lors que l'exposé des motifs ne précise rien à ce sujet et que l'article 106/20 en projet est lui-même très succinct, l'Autorité ne peut se prononcer de manière plus approfondie sur le projet et invite le demandeur à préciser le dispositif et l'objectif qu'il poursuit » (souligné par l'Autorité dans le texte original).

14. L'Autorité s'est encore positionnée récemment dans un sens similaire à ce qui vient d'être rappelé aux considérants nos 39-41 de son avis n° 115/2023 du 18 juillet 2023 *sur le projet d'arrêté royal portant modification de l'arrêté royal du 13 juin 2014 déterminant d'une part, les mesures réglementaires, administratives, techniques et organisationnelles spécifiques afin d'assurer le respect des prescriptions relatives à la protection des données à caractère personnel ou relatives à des entités individuelles et de secret statistique et d'autres part, fixant les conditions auxquelles l'Institut national de Statistique (INS) peut agir en qualité d'organisation intermédiaire en vue d'un traitement ultérieur à des fins statistiques. (CO-A-2023-213)*. L'article 203 de la LTD, se référant également au concept de tiers de confiance, dans le contexte des traitements à des fins archivistiques, de recherche scientifique ou historique, ou à des fins statistiques, prévoit que celui-ci doit être soumis au secret professionnel et être indépendant du responsable du traitement initial.

15. Dans un autre domaine que celui de l'anonymisation et de la pseudonymisation, le droit européen réglemente spécifiquement également, la prestation de certains services de confiance (dont la signature et l'horodatage électroniques)[9]. Ce cadre normatif peut également, *mutatis mutandis*, constituer une source d'inspiration pour le demandeur.

16. **L'Autorité est d'avis qu'à l'aune des considérations précédentes, le dispositif doit définir le concept de tiers de confiance certifié, en précisant les responsabilités, les qualités et garanties qui doivent assortir le prestataire, les prestations et la certification concernées,** en lien avec le traitement de données à caractère personnel. De telles dispositions ont en effet un impact direct sur la détermination d'éléments essentiels des traitements de données en question : elles participent à la détermination de la finalité du traitement envisagé (il s'agit de recourir à une entité

[9] Voir le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*.

spécifique, pour ses caractéristiques, afin de garantir la bonne exécution du traitement) et en assure la proportionnalité notamment en déterminant des garanties appropriées pour les droits et libertés des personnes concernées, et elles déterminent encore des responsabilités au regard du traitement de données à caractère personnel.

17. Plus concrètement, à l'aune des cadres normatifs précités, et sans préjudice des considérations que l'Autorité estimerait utile d'émettre à l'avenir à ce sujet, **l'Autorité est d'avis que les éléments suivants sont pertinents dans le cadre de la conception de telles dispositions et des réflexions en la matière**, sous réserve de la possibilité de leur mise en œuvre au regard du droit européen (ce qu'il appartient au demandeur de vérifier) :

- La fixation de **conditions relatives à la relation entre l'autorité publique concernée et le demandeur d'un côté, et le tiers de confiance de l'autre**. A ce sujet, le tiers de confiance devrait notamment être indépendant de l'autorité publique et du demandeur de la réutilisation ;

- La détermination des **responsabilités** des parties en cause au regard du traitement de données (pseudonymisation, anonymisation ou service d'accès sécurisé aux données). Notamment à ce sujet, compte-tenu de l'indépendance du tiers de confiance, de l'expertise spécialisée attendue de sa part ainsi que des obligations spécifiques qui lui incomberaient en la matière, du fait qu'il définira les caractéristiques essentielles (même s'il n'est pas exclu que l'autorité publique concernée soit également amenée à prendre certaines décisions dans le cadre de la mise en œuvre d'un processus d'anonymisation par exemple) des services qu'il offre, **l'Autorité est d'avis que le tiers de confiance devra être considéré comme le responsable conjoint du traitement** d'anonymisation ou de pseudonymisation des données, avec l'instance publique concernée ;

- La fixation de **conditions relatives au service offert/au traitement de données**. Par exemple, l'obligation de détruire les données une fois leur anonymisation réalisée peut être prévue, l'interdiction de principe des traitements de données en vue de réidentifier les personnes concernées, l'interdiction de traiter les données pour d'autres finalités, et l'obligation de rencontrer un niveau élevé de fiabilité. Dans ce contexte, l'Autorité est consciente de la difficulté d'assurer la mise en œuvre de garanties techniques et le cas échéant, procédurales également, dans le cadre d'un schéma de certification, élevées, et de permettre à la fois le développement de l'innovation en la matière, afin que les instances publiques puissent disposer d'une offre de services (de confiance) pertinente et suffisante. Il appartient au demandeur **d'assurer plus généralement que les conditions qu'il fixerait assurent le meilleur équilibre entre un niveau de garantie élevé et la possibilité d'innover et de**

développer des services en matière de pseudonymisation, anonymisation ou d'accès sécurisé aux données ;

- La détermination d'obligations en matière de **transparence**. De telles obligations peuvent par exemple concerner la déclaration/notification des tiers de confiance et publication de l'identité de ceux-ci, et la réalisation d'audits externes[10]. Plus fondamentalement, s'agissant de l'anonymisation, sont pertinentes des **obligations de transparence relatives aux processus d'anonymisation et aux mesures qui sont mises en œuvre pour limiter les risques de réidentification, ainsi que les compromis réalisés dans ce cadre** ;

- La fixation de **conditions relatives au prestataire de service tiers de confiance**. De telles conditions porteraient notamment sur son niveau **d'expertise** dans le cadre du traitement de données (pseudonymisation, anonymisation, accès sécurisé aux données), au regard de l'état de la technique, et sur sa capacité financière.

18. Troisièmement, l'exposé des motifs souligne qu'obtenir « *un **avis de l'Autorité** de protection des données sur le caractère approprié de la mesure dans* » le cas concret en question, constitue une « *garantie supplémentaire* » (gras ajouté par l'Autorité). Sur ce point, l'Autorité rappelle qu'elle n'est consultable que selon les modalités consacrées dans la LCA. A ce sujet d'une part, des demandes d'avis peuvent être introduites auprès du Centre de Connaissances de l'Autorité dans les conditions prévues à l'article 23 de la LCA (hypothèse du présent avis).

19. D'autre part, le Secrétariat général de l'Autorité peut également rendre un avis à l'attention d'un responsable du traitement, toutefois dans l'hypothèse limitée d'une analyse d'impact relative à la protection des données, à la suite d'une consultation par le responsable du traitement de l'Autorité de protection des données[11], lorsque le traitement concerné présente encore un risque résiduel élevé malgré les mesures de gestion des risques envisagés par le responsable du traitement[12].

20. En conclusion, **en exécution de la LCA, l'instance administrative saisie d'une demande de réutilisation ne peut pas de manière générale, soumettre à l'Autorité une demande d'avis quant au caractère approprié ou pas de la mesure envisagée**. Il appartiendra au responsable du traitement (l'instance administrative exécutant son obligation légale), conformément au principe

[10] Dans le domaine des élections sociales, voir par exemple le considérant n° 14 de l'avis n° 62/2023 du 9 mars 2023 *concernant un avant-projet de loi modifiant la loi du 4 décembre 2007 relative aux élections sociales, la loi du 20 septembre 1948 portant organisation de l'économie et la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail (CO-A-2023-030)*.

[11] Article 20, § 1er, 3°, de la LCA.

[12] Voir notamment https://www.autoriteprotectiondonnees.be/professionnel/actions/consultation-prealable-aipd, et le guide publié par l'Autorité à l'adresse suivante https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf, dernièrement consultés le 08/09/2023.

d'*accountability*, de déterminer et mettre en œuvre les mesures envisagées, et de pouvoir justifier de la conformité du traitement de données réalisé au regard du RGPD et de la loi de 2016 telle que modifiée par le Projet.

21. Quatrièmement, l'Autorité rappelle que de manière générale, **la loi de 2016 est sans préjudice du traitement ultérieur de données que pourrait réaliser un responsable du traitement qui a pu accéder à des données à caractère personnel conformément aux règles d'accès et dans les limites prévues par ces règles d'accès et par l'article 6, 4., du RGPD**. En d'autres termes, il appartiendra au demandeur (responsable de son traitement) de déterminer la voie juridique d'accès aux données concernées la plus appropriée, en fonction de son projet de traitement de données à caractère personnel : soit une simple demande d'accès ou une consultation des données conformément à la loi de 1994 (ou à une autre législation) ; soit une demande d'accès en vue d'une réutilisation des données conformément à la loi de 2016.

22. Cinquièmement, concernant la **définition de l'anonymisation** consacrée dans l'article 3, 16°, du Projet, l'exposé des motifs précise que « *Cette définition est alignée sur le sens donné à l'anonymisation dans le Règlement général sur la protection des données (Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel), qui est directement applicable en Belgique* ». L'Autorité relève que cette définition est la reprise littérale (à l'exception du concept de document qui est remplacé par celui de document « administratif ») de la définition consacrée dans l'article 2, 7), de la Directive elle-même. Le RGPD ne définit en effet pas le processus d'anonymisation. L'exposé des motifs peut être adapté en précisant que le Projet reprend la définition du processus d'anonymisation consacré dans la directive mais que cela étant précisé, la Directive est sans préjudice du RGPD, auquel elle renvoie par ailleurs concernant la définition du concept de données à caractère personnel, **et le traitement d'anonymisation de données devra être compris et interprété conformément au RGPD**.

23. Enfin sixièmement, tel que modifié par l'article 14 du Projet, l'article 9, § 1er, de la loi de 2016 prévoit que « *L'instance publique met à disposition les documents administratifs sous une forme et une langue préexistante sans que cela entraîne d'obligation de créer, d'adapter, ou de fournir des extraits de documents qui engendrerait des efforts disproportionnés dépassant le stade de la simple manipulation* » (souligné par l'Autorité). Comme l'indique l'exposé des motifs, cette disposition traite des formats dans lesquels les documents administratifs doivent être mis à disposition.

24. Dès lors que l'anonymisation ou la pseudonymisation de données nécessiteront en principe un traitement de données qui dépasse « le stade de la simple manipulation », **l'Autorité est d'avis que le Projet doit clarifier la relation entre l'obligation d'une instance publique** de mettre à disposition à des fins de réutilisation, des documents anonymisés ou pseudonymisés, **d'une part, et**

d'autre part, l'absence d'obligation de cette même instance de mettre des documents à disposition sous une forme qui engendrerait un effort disproportionné dépassant le stade de la simple manipulation. L'Autorité semble comprendre de la logique du dispositif du Projet que l'article 9, § 1er, de la loi de 2016 serait sans préjudice de l'obligation de l'instance de pseudonymiser ou anonymiser les documents concernés, dès lors que ces traitements peuvent être compensés par la répercussion de frais qu'ils engendrent, sur les demandeurs. Autrement dit, le fait que les efforts demandés à l'instance en la matière dépassent la simple manipulation, ne pourrait justifier le refus par l'instance concernée, de mettre à disposition des documents administratifs pseudonymisés ou anonymisés.

Par ces motifs,
L'Autorité est d'avis que

1. En exécution de la loi de 2016, des données à caractère personnel ne pourront être réutilisées que si l'accès à celles-ci est ouvert au grand public, sans nécessiter la justification d'un quelconque intérêt (**considérant n° 3**) ;

2. Le dispositif du Projet doit conformément au principe de minimisation des données, imposer le recours à l'anonymisation des données par l'instance publique avant d'en permettre la réutilisation ou, à défaut, si l'anonymisation ne permet pas d'accomplir la finalité de la réutilisation envisagée et pour autant que cela soit proportionné dans le cas d'espèce, la pseudonymisation des données à caractère personnel avant de permettre leur réutilisation (**considérants nos 7-9**) ;

3. Dans une perspective plus globale dans le domaine de la réutilisation des données, le demandeur devrait privilégier d'autres méthodes techniques permettant la réutilisation des données sans la communication des données pseudonymisées (ou rendues anonymes) aux demandeurs, via la mise à disposition de services sécurisés d'accès aux données, de manière telle que soit garanti un meilleur contrôle sur les traitements de données envisagés (**considérants nos 10-11**) ;

4. Le dispositif doit définir le concept de tiers de confiance certifié, en précisant les responsabilités, les qualités et garanties qui doivent assortir le prestataire, les prestations et la certification concernées, en lien avec le traitement de données à caractère personnel (**considérants nos 13-17**) ;

5. La LCA ne permet pas de manière générale, à l'instance publique de demander l'avis de l'Autorité quant à la mesure qu'elle envisage pour permettre la réutilisation des données (**considérants nos 18-20**) ;

6. La loi de 2016 est sans préjudice du traitement ultérieur de données que pourrait réaliser un responsable du traitement qui a pu accéder à des données à caractère personnel conformément aux règles d'accès et dans les limites prévues par ces règles et l'article 6, 4., du RGPD (**considérant n° 21**) ;

7. L'exposé des motifs du Projet peut être clarifié dans la mesure où c'est de la Directive elle-même qu'est repris le concept de processus d'anonymisation (**considérant n° 20**) ;

8. Le Projet doit clarifier l'impact de l'article 9, § 1er, de la loi de 2016 tel que modifié par l'article 14 du Projet, quant à l'obligation de mettre des données à disposition après anonymisation ou pseudonymisation (**considérants nos 23-24**).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière, Directrice