



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 115/2023 du 18 juillet 2023

Objet : Demande d'avis 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)

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 et Bart Preneel;

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 de Monsieur Pierre-Yves Dermagne, Vice-premier ministre et ministre de l'Economie et du Travail, reçue le 24 mai 2023 ;

Vu les informations complémentaires reçues en date du 13 juin 2023 ;

émet, le 18 juillet 2023, l'avis suivant :

I. Objet et contexte de la demande

1. Monsieur Pierre-Yves Dermagne, Vice-premier ministre et ministre de l'Economie et du Travail, sollicite l'avis de l'Autorité 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 (ci-après dénommé « le projet d'arrêté royal »).
2. Les principales modifications apportées par le projet d'arrêté royal à l'article 2 de l'arrêté royal précité de 2014 font suite à l'avis précité de l'Autorité n°127/2021¹ en ce qu'est actualisée la terminologie utilisée (notion de pseudonymisation en lieu et place de celle de « codage », de « clés de concordance » en lieu et place de celle de « clés logiques », ...) et en ce que ne sont (presque²) plus attribuées au délégué à la protection des données de l'INS des fonctions décisionnelles dans la réalisation des traitements de données nécessaires à l'exécution des missions de service public de l'INS. Pour autant que nécessaire, l'Autorité se prononce également dans le présent avis sur les dispositions de l'Arrêté royal précité de 2014 qui ne font pas actuellement l'objet de modifications.
3. L'Autorité a rendu deux avis récents sur les projets de modification de la loi précitée du 4 juillet 1962 qui ont abouti à la loi précitée du 25 septembre 2022³. Etant donné que ces avis contiennent des recommandations en matière de mesures organisationnelles et techniques à adopter dans le cadre de la réalisation de statistiques publiques, l'auteur du projet d'arrêté royal y est renvoyé pour les aspects non couverts par le présent avis.

¹ Avis 127/2021 du 28 juillet 2021 sur l'avant-projet de loi modifiant la loi du 4 juillet 1962 relative à la statistique publique.

² Cf. infra.

³ A savoir, l'avis 127/2021 du 28 juillet 2021 sur l'avant-projet modifiant la loi du 4 juillet 1962 relative à la statistique publique et l'avis 32/2022 concernant les articles 7, 25, 1° et 47 du projet de loi portant dispositions diverses en matière d'Economie. Ce dernier avis concerne la loi fédérale statistique publique en ce qu'il porte sur l'habilitation législative conférée à l'INS de se voir communiquer des données de trafic et de localisation des abonnés que les opérateurs sont tenus de conserver en vertu des articles 122 et 123 de la loi du 13 juin 2005 relative aux communications électroniques.

II. Examen

a. Chapitre 1^{er} de l'AR en projet intitulé « mesures réglementaires, administratives, techniques et organisationnelles de référence applicables à tout traitement de données.

i. Caractère minimal des mesures imposées

4. Le chapitre 1^{er} de l'arrêté royal en projet dresse une liste de mesures qui s'imposent à l'INS pour la sécurisation des traitements de données qu'il réalise dans l'exercice de ses missions et ce, en exécution de l'article 17quater de la loi précitée de 1962 qui délègue au Roi le soin de « *fixer les modalités réglementaires, administratives, techniques et organisationnelles spécifiques afin d'assurer le respect des prescriptions relatives à la protection des données individuelles à caractère personnel ou relatives à des entités individuelles et de secret statistique* ».
5. Même si l'imposition de telles mesures est indiquée au titre de la protection des données à caractère personnel au vu des risques importants pour les droits et libertés des personnes concernées que génèrent les activités des organismes en charge de la statistique publique (en raison des risques que les traitements de données que ces activités génèrent tant du point de vue de l'ampleur des personnes concernées que de la masse et du niveau de détail des données les concernant qui sont traitées et des couplages de bases de données que ces activités nécessitent), l'Autorité relève qu'il ne peut être question de dresser une liste exhaustive de telles mesures étant donné que c'est au responsable du traitement, à savoir l'INS, qu'il appartient d'opter pour des mesures techniques et organisationnelles adéquates et appropriées en fonction des risques spécifiques générés par les traitements spécifiques de données qu'il réalise au gré de ses programmes statistiques et des requêtes auxquelles il doit répondre en exécution de l'article 15 de la loi précitée de 1962. Lesdites mesures devant toujours également être adaptées au vu de l'état actuel des règles de l'art en la matière et de l'évolution de la technique (art. 25 RGPD). Par conséquent, il est recommandé d'adapter le titre de l'AR ainsi que du chapitre 1^{er} en prévoyant en lieu et place une énumération d'une liste des mesures minimales à prendre par l'INS.

ii. Politique écrite de sécurité

6. Au niveau de l'article 1^{er} en projet et pour les mêmes motifs que ceux explicités ci-avant, il convient de prévoir l'obligation pour l'INS de mettre continuellement à jour sa politique écrite de sécurité. Cette politique constitue pour l'INS un moyen de se conformer à son obligation d'accountability consacrée à l'article 24 du RGPD qui prévoit que tout responsable du traitement est tenu de « *mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD* ».

iii. Mesures techniques minimales

7. L'article 2 en projet de l'AR prévoit une liste de mesures spécifiques que doit adopter l'INS. L'auteur de l'AR en projet les qualifie de techniques, d'organisationnelles et de juridiques.
8. Selon le libellé de l'article 2, al.1, 1° en projet, les mesures techniques⁴ consistent en « *la classification des données, la gestion des accès aux données classifiées, les mesures particulières pour les données à caractère personnel avec identifiants directs, l'information et la formation du personnel, la pseudonymisation des données, la protection des clefs de concordance permettant de réassocier les données d'étude aux données d'identification directe* ». La suite de cette disposition en projet précise en quoi consistent chacune desdites mesures.
9. Tout d'abord, l'Autorité relève à ce sujet qu'il convient de définir les concepts utilisés qui ne sont pas déjà définis par la loi précitée de 1962, à savoir la notion d'identifiant direct.
10. La détermination de niveaux de classification de données liés (i) au degré d'identifiabilité des personnes concernées et au (ii) degré de sensibilité des informations les concernant constitue une mesure adéquate. Il s'agit en effet de critères pertinents pour apprécier l'ampleur du risque que représente un traitement pour les personnes concernées. Le niveau de sécurité à atteindre pour chaque traitement doit être proportionné à ce niveau de risque.
11. L'Autorité est d'avis que cette conséquence doit ressortir plus clairement du point 1.1 de l'article 2 en projet qui actuellement ne fait que dresser les différents niveaux de classification sans les qualifier et prévoit uniquement que « *la classification des informations définit le niveau de protection des données* ».
12. De plus, il convient de prévoir que même des données à caractère personnel pseudonymisées sensibles au sens des articles 9 et 10 du RGPD nécessitent de plus amples mesures de protection que des données à caractère personnel pseudonymisées qui ne présentent pas ces caractéristiques.
13. Enfin, il convient également de définir dans l'arrêté royal en projet les notions de «données globales » et de «données anonymes » qui sont reprises dans cette classification.

⁴ Lesquelles doivent être qualifiées de minimales (cf. supra).

14. Concernant la notion de "donnée anonyme", l'Autorité rappelle que l'anonymisation de données à caractère personnel ne consiste pas uniquement à leur ôter les informations qui permettent d'identifier directement les personnes sur lesquelles elles portent (nom, prénom, numéro d'identification unique, adresse, ...) mais également les informations qui permettent de les identifier par un processus d'individualisation, de corrélation ou d'inférence. Il convient donc d'intégrer dans le projet d'arrêté royal une définition de cette notion qui révèle ce standard élevé requis.
15. Quant à la notion de « données globales », l'Autorité comprend que l'auteur de l'arrêté royal en projet vise la notion de données agrégées étant donné que, comme l'Autorité a déjà eu l'occasion de le rappeler⁵, le terme généralisation est utilisé pour se référer au processus technique visant à rendre les données d'une personne concernée moins précise (par exemple, remplacer sa date de naissance par son âge, son adresse par un ZIP code) ; ce qui n'empêche que les données généralisées se réfèrent toujours à une seule personne et constituent toujours des données à caractère personnel si la ou les personnes sur lesquelles elles portent sont identifiée ou identifiables au sens de l'article 4.1 du RGPD. A l'inverse, l'agrégation se réfère au processus technique consistant à regrouper les informations concernant plusieurs personnes de manière telle que chaque donnée se réfère au moins à un groupe de personnes. Par exemple, l'information reprenant le nombre de personnes ayant voyagé de Liège à Bruxelles à une date spécifique ou le nombre de femmes qui vivent dans une commune spécifique sont des données agrégées⁶. L'autorité recommande donc de remplacer la notion de « données globales » par celle de « données agrégées » et de la définir conformément aux développements qui précèdent.
16. Quant aux mesures que l'INS doit adopter en matière de gestion des accès aux données autres que les données « *globales et anonymes* », il est recommandé que l'arrêté royal en projet soit plus prescriptif. Prévoir que les accès « *sont gérés au plus près* », c'est-à-dire qu'ils ne soient « *accordés qu'aux personnes ayant le besoin d'en connaître* » semble insuffisant. A ce sujet, l'article 17 de la loi précitée de 1962 prévoit déjà, à la suite de l'avis précité de l'Autorité n° 127/2021, que seuls les agents de l'INS en charge de la collecte des données et ceux en charge des opérations de contrôle de qualité et, le cas échéant, de couplage peuvent avoir accès aux données à caractère personnel avec identifiants directs. Afin de cadrer plus adéquatement les exigences minimales requises en matière de gestion des accès des données collectées par l'INS, il est nécessaire d'une part, de lier explicitement le besoin d'en connaître avec la finalité concrète poursuivie par l'agent en charge d'une étude statistique spécifique ainsi qu'avec son domaine d'activité particulier⁷, cette finalité délimitant tant

⁵⁵ Cf. à ce sujet, les considérants 53 et s. de l'avis 35/2023 du 9 février 2023 sur le projet de décret introduisant dans le Code wallon de l'Action sociale et de la santé des dispositions relatives aux programmes de médecine préventive

⁶ Des données agrégées peuvent être considérées comme anonymes selon les paramètres d'agrégation et le cas échéant l'ajout de bruit.

⁷ À l'instar de ce que prévoit le règlement européen 553/2013 relatifs aux statistiques européennes.

l'ampleur des données à accéder que la période de temps nécessaire pendant lequel cet accès doit être accordé. D'autre part, il convient également de prévoir explicitement que la gestion desdits accès se fera en conformité avec l'article 17 de la loi précitée de 1962.

17. Ensuite, l'Autorité relève que les demandes d'accès ne doivent pas être validées par le délégué à la protection des données (étant donné qu'il s'agit d'une fonction décisionnelle dans la réalisation du traitement de données qui n'est pas de son ressort au vu des articles 38 et 39 du RGPD) mais peuvent intervenir après avis de ce dernier.
18. De plus, au vu de la sensibilité que présente l'accès aux clefs de concordance qui permettent de retrouver l'identité des personnes à propos desquelles l'INS a pseudonymisé des données, l'Autorité recommande d'imposer à l'INS des mesures de journalisation d'accès spécifiques auxdites clefs. Elle renvoie à ce sujet à son avis précité de 2021 dans lequel elle recommandait de déterminer explicitement dans la réglementation les types de fonction au sein de l'INS qui peuvent avoir à ces clefs et la tenue obligatoire par l'INS d'une journalisation des accès à ces clefs décrivant qui y a eu accès, quand et pourquoi concrètement. A défaut de l'avoir prévu dans la loi précitée de 1962, il convient de le faire dans le projet d'arrêté royal.
19. Le point 1.3 de l'article 2 de l'arrêté royal précité de 2014 traite des « *mesures particulières pour les données avec identifiants directs* ». Cette disposition traitant des mesures de journalisation des accès à ce type de données n'est pas adaptée par le projet d'arrêté royal. L'Autorité relève à ce sujet que, les données pseudonymisées étant toujours des données à caractère personnel, il est indiqué qu'elles soient également couvertes par cette obligation de journalisation des accès qui est imposée à l'INS ; d'autant plus qu'il rentre dans les missions de l'INS de communiquer des données pseudonymisées à une série de destinataires énumérés à l'article 15 de la loi précitée de 1962 ; quitte, pour l'INS, à intégrer des engagements en ce sens de la part desdits destinataires dans le contrat de confidentialité qui doit être conclu en vertu de l'article 15bis de cette loi de 1962 ; ce qui permettrait également à l'INS de vérifier le respect par ces destinataires des principes statistiques d'impartialité, d'objectivité et d'indépendance professionnelle visés à l'articles 1erbis, al.1, 4° de la loi précitée de 1962. A titre plus fondamental, l'Autorité relève qu'aucune mesure n'est prévue par le projet d'arrêté royal pour sécuriser les communications de données pseudonymisées réalisées par l'INS en exécution de l'article 15 de la loi précitée de 1962. A ce sujet, l'Autorité attire l'attention du législateur sur le fait qu'il est plus conforme aux principes de protection des données de prévoir que ces communications de données aient lieu au sein du système d'information de l'INS (via un data room spécifiquement configuré à cette fin) afin que les données pseudonymisées ne quittent pas la « data room » de l'INS. Il importe en effet que l'INS puisse garder le contrôle de l'utilisation qui est faite de ces données ; ce qui permet de diminuer le risque de détournement de finalité desdites données. L'Autorité recommande vivement de prévoir une disposition en ce sens dans le projet d'arrêté royal.

20. Quant au niveau de qualité de la journalisation qu'il est exigé de l'INS, il est recommandé d'intégrer dans cette journalisation obligatoire la mention de l'étude statistique ou du dossier spécifique (numéro de dossier) pour lequel les requêtes sur les données à caractère personnel ont été effectuées. Sans cette information, il est en effet impossible de détecter l'existence des requêtes excessives pour une tâche spécifique ou encore un éventuel détournement de finalité
21. Enfin, toujours au niveau du point 1.3 de l'article 2 de l'arrêté royal en projet, il est recommandé d'imposer à l'INS de mettre en place un système automatisé de détection des accès anormaux aux données à caractère personnel (par exemple en fonction de leur fréquence anormale et de leur ampleur anormale).
22. Le point 1.4 de l'article 2 de l'AR précité de 2014 traite de l'information et de la formation du personnel de l'INS. Il est indiqué de prévoir que la sensibilisation du personnel porte non sur la sécurité de l'information mais sur la protection des données à caractère personnel (dans laquelle est incluse la sécurité de l'information) en ce compris les garanties pour les droits et libertés des personnes concernées reprises dans la loi précitées de 1962.
23. Le point 1.5 traite de la pseudonymisation des données. Le projet d'AR remplace la disposition actuelle en prévoyant que :
« les données sont traitées de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »
24. Tout d'abord, l'Autorité s'interroge si la finalité de garantir que les données ne sont pas attribuées à une personne identifiable ne procède pas d'une erreur étant donné que par nature une donnée pseudonymisée est donnée relative à une personne identifiable étant donné que des informations complémentaires (à savoir la clé de concordance ou, plus généralement, le secret de pseudonymisation) permet de réidentifier la personne.
25. De plus, l'Autorité relève que cette disposition en projet ne détermine pas à suffisance sur quelles données elle porte. Viser « les données » sans autre précision n'apporte pas la prévisibilité et la sécurité juridique requise. Selon la compréhension de l'Autorité, il s'agit de l'hypothèse de réalisation par l'INS de projets de statistiques publiques qui ne peuvent être poursuivis qu'au moyen de données pseudonymisées ou encore de réponses par l'INS à des requêtes d'accès qui lui sont faites en vertu de l'article 15 de la loi précitée de 1962 et qui ne peuvent également être satisfaites qu'avec de telles données. Cela mérite d'être précisé.

26. Il est également recommandé d'ajouter au point 1.5 que l'INS opte pour la technique ou la combinaison de techniques les plus appropriées et les plus conformes aux règles actuelles de l'art pour minimiser les risques pour les personnes concernées et documente ses choix par écrit, pour chaque projet de statistiques publiques ou pour chaque requête d'accès pertinente⁸. A ce sujet, il est renvoyé aux développements de l'Autorité repris dans son avis précité de 2021⁹. En particulier, l'INS veillera à une minimisation stricte des données traitées conformément à ce que requiert l'article 5.1.c du RGPD.
27. Ensuite, l'Autorité relève que l'AR précité de 2014 ne traite que des mesures de pseudonymisation de données alors que certaines études statistiques peuvent être réalisées au moyen de données anonymes¹⁰. Il convient donc de prévoir dans le projet d'arrêté royal un point spécifique relatif aux procédures d'anonymisation de l'INS et d'utilisation dans ce cadre de dispositifs conformes aux règles actuelles de l'art et adéquatement documentés par écrit.
28. En outre, il est indiqué de prévoir explicitement qu'en tout état de cause l'INS met en place toutes les mesures appropriées pour éviter de devoir conserver des données d'identification des personnes concernées. A cet égard, l'Autorité renvoie à son avis précité de 2021¹¹.
29. Le point 1.6 de l'article 2 de l'AR précité de 2014, relatif à la protection des clés de concordance, est également adapté pour prévoir dorénavant que
- « Par mesure de sécurité, les clés de concordance sont chiffrées lorsque leur archivage est nécessaire. Le déchiffrement des clés de concordance ne peut se faire qu'après avis du délégué à la protection des données »*
30. En plus des mesures recommandées ci-dessus en matière de journalisation des accès aux clés de concordance, il convient de prévoir, ainsi que cela a été explicité par l'Autorité dans son avis précité de 2021, que l'INS préserve le secret de pseudonymisation utilisé¹² au moyen de mesures techniques et organisationnelles adéquates qui dépendent du scénario de pseudonymisation utilisé, lesquelles impliquent notamment la séparation physique du secret de par rapport aux données d'études ainsi que la suppression du secret de pseudonymisation de tout support de stockage à risque. En outre, il convient de préciser que le chiffrement des secrets de pseudonymisation est réalisé selon les règles actuelles de l'art en cas de conservation automatisée avec un stockage et une gestion des clés adaptés au type de chiffrement utilisé.

⁸ Càd, qui nécessite de traiter/communiquer des données pseudonymisées et qui ne peut se satisfaire de données anonymisées.

⁹ Cf. notamment les considérants 7 et 34

¹⁰ Cf à ce sujet les développements de l'Autorité dans son avis précité de 2021 repris aux considérants 45 et suivants

¹¹ Cf. notamment les recommandations de mesures permettant d'éviter de conserver les données des non-répondants aux enquêtes de l'INS tout en parvenant à ne plus contacter ces personnes lors d'une enquête ultérieure.

¹² étant donné que la pseudonymisation des données peut être réalisée par d'autre technique que le codage

31. Concernant le point 1.7 relatif à la pseudonymisation des données communiquées dans le cadre de l'article 15 de la loi précitée de 1962, l'Autorité renvoie à ses considérations qui précèdent à ce sujet. Pour le surplus, l'Autorité s'interroge sur l'ajout du terme « notamment » au niveau de la détermination des circonstances dans lesquelles une même unité statistique se verra attribuer un pseudonyme identique pour plusieurs communications faites en exécution de l'article 15 de loi précitée de 1962, à savoir, « *lorsque le suivi des unités au cours du temps est requis (enquêtes par panel et études longitudinales)* ». A défaut de justification spécifique dûment motivée à reprendre dans le rapport au Roi, il convient de supprimer le terme « notamment ». En outre, l'Autorité s'interroge également en quoi la réalisation d'enquêtes par panel sans caractère longitudinal nécessite une telle façon de procéder. A défaut de justification à ce sujet dans le rapport au Roi, il convient également de supprimer la référence à cet exemple.

iv. Mesures organisationnelles minimales

32. Le point 2° de l'article 2 de l'AR précité de 2014 dresse la liste des mesures organisationnelles adoptées par l'INS. En raison des motifs explicités ci-dessus, il convient de préciser qu'il s'agit des mesures minimales.
33. Le point 3° de ce point 2° de l'article 2 en projet prévoit que « *l'INS veille au contrôle de l'utilisation des clés de concordance permettant la réidentification des données, pour éviter tout risque d'utilisation à des fins autres que statistiques ou de recherche scientifique* ». Pour les motifs explicités ci-dessus, il convient de viser les clefs de concordance et/ou tout autre secret de pseudonymisation utilisé pour pseudonymiser les données. De plus, en lieu et place de viser de manière générale toutes fins autres que statistiques ou de recherche scientifique, il convient, dans le respect du principe de finalité et au titre de garantie pour les droits et libertés des personnes concernées, de préciser qu'il ne peut s'agir de fins autres que les fins concrètes statistiques ou de recherche scientifique pour lesquelles les données ont été pseudonymisées.
34. L'Autorité relève que la sécurisation de la configuration des clés de concordance et le contrôle de leur utilisation doivent nécessairement s'accompagner d'une veille par l'INS au niveau de la constitution des tables de données pseudonymisées mises à disposition de ses services thématiques en charge de la réalisation des statistiques. En effet, il convient de veiller, d'une part, à éviter que ces différentes tables soient composées d'un nombre de catégories identiques de données (relatives à des mêmes personnes) supérieur à 15¹³ (dans l'hypothèse où plusieurs tables sont mises à leur disposition) et,

¹³ Il a notamment été montré que 15 attributs démographiques étaient suffisants pour ré-identifier une personne de manière unique. Rocher, L., et al. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications, 10(1), pp.1-9. <https://www.nature.com/articles/s41467-019-10933-3>;

d'autre part, d'assurer un respect strict du principe de minimisation du RGPD dans la constitution de ces tables. L'Autorité recommande d'ajouter une mesure organisationnelle en ce sens dans le projet d'arrêté royal.

v. Mesures juridiques

35. Quant aux mesures juridiques énumérées au point 3° de l'article 2 en projet, les modifications apportées sont de pure forme. L'Autorité considère que le devoir de confidentialité et l'obligation de secret statistique doivent être imposés non seulement aux agents de l'INS mais également à tout sous-traitant auquel l'INS ferait appel¹⁴ ainsi qu'aux personnes qui se voient communiquer de la part de l'INS des données pseudonymisées en exécution de l'article 15 de la loi précitée de 1962. En outre, à titre de garantie pour les personnes concernées, il est indiqué de prévoir explicitement que ce devoir de confidentialité est d'application même après la cession des fonctions.

b. Chapitre 2 du projet d'AR traitant des conditions auxquelles l'INS peut agir en qualité d'organisation intermédiaire en vue d'un traitement ultérieur à des fins statistiques (art. 3 à 5)

36. Le chapitre 2 du projet d'AR traite des conditions auxquelles l'INS peut agir en qualité d'organisation intermédiaire en vue du traitement ultérieur à des fins statistiques, en exécution de l'article 17quater, §2 de la loi précitée de 1962.

37. L'Autorité constate l'absence de détermination claire de ce en quoi consiste cette mission de service public de l'INS dans la loi précitée de 1962 (ce à quoi il conviendrait également de pallier). Ainsi qu'il ressort de l'arrêté royal précité de 2014, l'objet de la mission confiée à l'INS en tant qu'organisation intermédiaire consiste à coupler des bases de données tant externes qu'internes¹⁵ sans plus de précisions en vue de générer des données pseudonymisées. A nouveau, l'Autorité relève l'omission de la référence au fait de générer des données anonymisées ; ce à quoi il convient également de pallier.

38. Sous réserve de la position du Conseil d'Etat, il convient qu'une évaluation préalable soit faite quant à la compatibilité pour l'INS de réaliser ces types de prestations de services en tant qu'organisation intermédiaire avec la réglementation européenne en matière statistiques publique, vu son statut d'autorité statistique nationale.

¹⁴ Pour autant qu'ils répondent aux critères requis en matière de formation et de qualification du personnel, conformément à ce que requiert le code européen de bonne conduite en matière de statistiques publiques. Des exigences de ce types pourraient d'ailleurs être ajoutées au niveau des mesures organisationnelles.

¹⁵ L'autorité renvoie à ce sujet à ses développements repris au considérant 58 de son avis précité 127/2021.

39. D'un point de vue strict de protection des données, un organisme intermédiaire qui procède à l'anonymisation ou à la pseudonymisation de données en vue de les communiquer à des fins de recherche statistiques est un tiers de confiance au sens des articles 202 et suivants de la LTD et doit donc présenter les garanties visées (soumission au secret professionnel et garantie d'indépendance par rapport aux responsables du traitement initiaux qui ont collecté les données et aux responsables de traitements ultérieurs qui vont réaliser les études statistiques) et disposer d'une expertise en technique de protection des données.
40. L'intervention d'un organisme intermédiaire dans le cadre de ce type de traitements à risques (en ce qu'ils impliquent des couplages de base de données) constitue une garantie pour les personnes concernées étant donné que le risque de dépseudonymisation diminue vu que le secret de pseudonymisation est gardé par ce tiers de confiance¹⁶.
41. Comme la Commission de protection de la vie privée, prédécesseur en droit de l'Autorité, l'a déjà mis en évidence, un tel tiers de confiance ne peut pas utiliser les données qu'il collecte pour prêter ses services de confiance (pseudonymisation, couplage, anonymisation) pour d'autres finalités que les finalités spécifiques de couplage et de pseudonymisation ou d'anonymisation qui lui ont été confiées¹⁷. Permettre à l'INS de réutiliser les données qu'il a traitées pour réaliser une de ses missions spécifiques d'organisation intermédiaire et ce, pour ses propres finalités génériques de statistiques publiques pose question non seulement au regard du principe de finalité du RGPD et des risques engendrés pour les droits et libertés des personnes concernées de telles centralisations et réutilisations massives de données (eu égard à la masse et au niveau de détail très important des données concernées) mais également, au regard du principe de finalité statistique consacré à l'article 1bis de la loi précitée de 1962 en vertu duquel « *des données collectées pour une fin statistique déterminée ne peuvent être utilisées à d'autres fins statistiques que si ces dernières sont compatibles avec la finalité statistique originaire* ».
42. De plus, sous réserve de la position du Conseil d'Etat, l'Autorité s'interroge aussi quant à la compatibilité d'une telle réutilisation avec les exigences d'indépendance professionnelle de toute

¹⁶ Cf. art. 202, §2 de la LTD.

¹⁷ Cf. à ce sujet la recommandation 02/2010 du 31 mars 2010 de la CPVP concernant le rôle de protection de vie privée des Trusted third parties (TTP ou tiers de confiance) lors de l'échange de données, p. 6. Dans cette même recommandation, il est d'ailleurs mis en évidence le fait que ce « *tiers de confiance doit détruire les données à caractère personnel qui lui ont été transmises par les responsables du traitement initiaux dès qu'il a accompli sa mission d'anonymisation, moins qu'il ne s'agisse d'une mission dont il découle qu'il doit conserver les données* ».

autorité statistique tant vis-à-vis du secteur public que du secteur privé à partir du moment où l'INS a un intérêt propre dans les données qu'il traite en tant qu'organisation intermédiaire¹⁸.

43. Au vu de ce qui précède, il convient donc d'adapter les articles 3 et 5 de l'arrêté royal précité de 2014 pour y préciser (i) que cette mission d'organisation intermédiaire ne peut être assurée par l'INS que lorsqu'elle est nécessaire en cas de requête visée à l'article 15 de la loi et (ii) pour y supprimer la possibilité pour l'INS de réutiliser pour ses propres besoins les données collectées pour ces tiers dans le cadre de cette prestation de services. La notion de tiers utilisée à l'article 3 de l'arrêté royal en projet mérite également d'être précisée en visant les tiers visés à l'article 15 de la loi précitée de 1962. Une fois les couplages pour les tiers réalisés, les données doivent donc être détruites conformément au statut de tiers de confiance des organisations intermédiaires. Il convient également de le préciser.
44. Il va également de soi que si l'INS réalise de tels traitements de couplage, pseudonymisation et anonymisation, il devra être qualifié de responsable du traitement desdites opérations de traitements de couplage, pseudonymisation et anonymisation. Cela mérite d'être précisé dans l'arrêté royal en projet.
45. En outre, l'Autorité recommande l'intervention du législateur pour consolider ce statut de tiers de confiance en encadrant adéquatement ce type de prestataires de services. Un minimum d'obligations spécifiques doit en effet leur être imposées au titre de garanties pour les droits et libertés des personnes concernées vu les risques spécifiques pour la protection des données que ces activités de couplages de bases de données variées et de traitements à grande échelle que ces activités engendrent ainsi que pour garantir la qualité des services qu'ils présentent dans ce cadre. Il est recommandé que l'auteur du projet entame une réflexion à ce sujet. Une source d'inspiration partielle peut éventuellement être trouvée dans les dispositions du Règlement européen Eidas¹⁹ qui encadre d'autres types de tiers de confiance.
46. Concernant l'article 4 de l'arrêté royal précité de 2014, il est renvoyé aux remarques faites ci-dessus sur l'article 2, al. 1, 2^o, *litera* 3^o qui s'appliquent *mutatis mutandis*.

¹⁸ Sur la question de la durée de conservation par l'INS données qu'il collecte dans l'exercice de ses missions, l'Autorité renvoie à ses développements repris aux considérants 56 et suivant de son avis précité n° 127/2021 lesquelles mettent notamment en évidence que « *si l'INS vient à ne jamais effacer les données à caractère personnel qu'il collecte et pseudonymise sans ne jamais détruire les clefs de pseudonymisation utilisées, cela implique une centralisation permanente par l'INS d'une masse énorme de données à caractère personnel diversifiées sur la population belge ; ce qui représente une ingérence importante dans le droit à la protection des données des personnes concernées qui pose question au regard de l'article 1bis de la loi relative à la statistique publique et des principes de finalité et de proportionnalité du droit à la protection des données. Même si le RGPD permet la réalisation de traitements ultérieurs à finalité d'études statistiques et de recherches scientifiques, le respect du principe de finalité implique que les modalités d'un traitement ultérieur de données soient limitées au strict nécessaire pour la réalisation de cette étude statistique ou de cette recherche scientifique ultérieure* ».

¹⁹ 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

Par ces motifs,**L'Autorité,****Considère que l'avant-projet doit être adapté en ce sens:**

1. Précision que les mesures imposées à l'INS sont des mesures minimales (cons. 4 et 5 et 32) ;
2. Imposition à l'INS de mise à jour de sa politique écrite de sécurité (cons. 6) ;
3. Ajout des définitions de certains concepts utilisés pour assurer un niveau correct de sécurité juridique (cons. 9 et 13 à 15) ;
4. Précisions des mesures requises pour la gestion des accès aux données traitées par l'INS, en ce compris de la détermination du niveau requis de qualité des mesures de journalisation des accès tant aux données qu'aux clefs de concordance, conformément aux considérants 16 à 20 ;
5. Suppression de l'attribution au délégué à la protection des données de l'INS de fonction décisionnelle dans la réalisation des traitements de données (cons. 17 et 46) ;
6. Imposition à l'INS de mettre en place un système de détection automatisée des requêtes d'accès anormales aux données (cons. 21) ;
7. Inclusion de la protection des données dans les matières sur lesquelles le personnel de l'INS en charge des traitements de données à caractère personnel doit être formé (cons. 22) ;
8. Adaptation de l'article 15 en projet traitant de la pseudonymisation des données par l'INS conformément aux considérants 24 à 26 ;
9. Inclusion du processus d'anonymisation dans les mesures à prendre par l'INS (cons. 27 et 28 et 37) ;
10. Inclusion de mesures spécifiques devant entourer la protection des clefs de concordance (cons. 30 et 33) ;
11. Ajout d'une mesure organisationnelle imposant à l'INS d'assurer une veille quant à la configuration des tables de données mises à disposition de ses services thématiques pour qu'elle présentent les garanties requises explicitées au considérant 34 ;
12. Adaptation de l'article 17 en projet qui traite de la pseudonymisation des données communiquées par l'INS en exécution de l'article 15 de la loi précitée de 1962 conformément au considérant 31 ;
13. Augmentation des catégories de personnes soumises au devoir de confidentialité et à l'obligation de secret statistique ainsi que de la période pendant laquelle elles y restent soumises (cons. 35) ;
14. Clarification du contenu de la mission d'organisation organisation intermédiaire confiée à l'INS tant dans la loi précitée de 1962 que dans le projet d'arrêté royal (cons. 37 et 38 et 43) et soumission d'obligations légales spécifiques à ce type d'intermédiaire pour assurer tant l'existence de garanties spécifiques pour les personnes concernées dans l'exercice de ce type de tâches qui impliquent des couplages de bases de données variées et traitements à grande échelle de données qu'une garantie de qualité des services prestés de tiers de confiance (cons. 45) ;

15. Suppression des dispositions qui permettent à l'INS de réaliser des traitements de données incompatibles avec son statut de tiers de confiance (réutilisation des données collectées pour des tiers pour ses propres besoins (cons. 41 à 43) ;
16. Précision que l'INS agit en tant que responsable du traitement dans la réalisation des traitements de données de couplage, pseudonymisation et anonymisation réalisée en tant qu'organisme intermédiaire lorsqu'il répond aux requêtes des tiers visés à l'article 15 de la loi précitée de 1962 (cons. 44).

Pour le Centre de Connaissances,
(s) Cédric Morlière, Directrice